CANADIAN JOURNAL OF MATHEMATICS

Journal Canadien de Mathématiques

VOL. XII - NO. 1
1960

Published for
THE CANADIAN MATHEMATICAL CONGRESS
by the
University of Toronto Press

The chief languages of the *Journal* are English and French.

Manuscripts for publication in the *Journal* should be sent to the *Editor-in-Chief*, G. F. D. Duff, University of Toronto. Authors are asked to write with a sense of perspective and as clearly as possible, especially in the introduction. Regarding typographical conventions, attention is drawn to the Author's Manual of which a copy will be furnished on request.

All other correspondence should be addressed to the *Managing Editor*, G. de B. Robinson, University of Toronto.

The *Journal* is published quarterly. Subscriptions should be sent to the *Managing Editor*. The price per volume of four numbers is $10.00. This is reduced to $5.00 for individual members of recognized Mathematical Societies.

The Canadian Mathematical Congress gratefully acknowledges the assistance of the following towards the cost of publishing this Journal:

University of Alberta
University of British Columbia
Dalhousie University
Université Laval
University of Manitoba
McMaster University
Mount Allison University
Queen's University
University of Saskatchewan
Assumption University
Carleton College
Ecole Polytechnique
Loyola College
McGill University
Université de Montréal
Nova Scotia Technical College
St. Mary's University
University of Toronto
National Research Council of Canada
and the
American Mathematical Society

AUTHORIZED AS SECOND CLASS MAIL, POST OFFICE DEPARTMENT, OTTAWA

SUR QUELQUES SÉRIES DE LAMBERT ET DE DIRICHLET

JACQUES TOUCHARD

Introduction. Nous nous occupons dans ce travail de séries dont voici le type le plus simple

$$\sum_{k=1}^{\infty} a_k \frac{x^k}{1-x^k}\frac{y^k}{1-y^k}$$

et de leurs analogues lorsqu'on remplace x^n par n^{-s} et y^n par $n^{-s'}$. Faute d'une autre désignation, nous avons cru pouvoir appeler ces séries respectivement séries de Lambert et séries de Dirichlet. Une série plus générale que la précédente est

$$\sum_{k=1}^{\infty} a_k \frac{g(x^k)}{1-x^{2\omega k}}\frac{g(y^k)}{1-y^{2\omega k}}$$

où les a_k sont des constantes et où $g(x)$ est un polynôme dont les coefficients sont des symboles de Jacobi (**1**, pp. 132-40; **4** pp 361–9).

$$\chi(n) = \left(\frac{D}{n}\right)$$

possédant la période 2ω.

Les expressions

$$g\left(e^{\frac{2\pi i m}{2\omega}}\right)$$

ont des propriétés multiplicatives analogues à celles des sommes de Ramanujan (**6**) d'où l'on peut déduire deux propositions concernant les racines de $g(x)$. Nous nous bornerons à les énoncer, dans les §§ 6 et 7, car elles résultent des calculs effectués autrefois par Dirichlet (**2**, pp. 46–50, 188–93), dans ses recherches sur le nombre des classes de formes quadratiques binaires d'un déterminant donné. Les polynômes $g(x)$ sont donc loin d'être nouveaux. Nous les avons utilisés toutefois, dans les §§ 10 et 11, pour obtenir des séries analogues à une belle série de Ramanujan. Dans les §§ 13 et 14, nous avons donné la représentation par des intégrales définies de diverses fonctions examinées auparavant.

1. Séries de Lambert. Soit $\chi(n)$ une fonction arithmétique complètement multiplicative, c'est-à-dire telle que $\chi(m)\cdot\chi(n) = \chi(m\ n)$, quels que soient

Reçu le 10 août, 1958.

les entiers positifs m et n. Désignons par $A(x)$ la série supposée convergente

$$A(x) = \sum_{n=1}^{\infty} \chi(n) x^n \tag{1}$$

et soit

$$G(x, y) = \sum_{k=1}^{\infty} a_k A(x^k) A(y^k), \tag{2}$$

où les a_k sont des coefficients constants. Quel est le terme en $x^\lambda y^\mu$ au second membre de (2)? Comme

$$a_k A(x^k) A(y^k) = a_k \sum_{h=1}^{\infty} \sum_{h'=1}^{\infty} \chi(h) \chi(h') x^{hk} y^{h'k} \tag{3}$$

on n'aura $hk = \lambda$, $h'k = \mu$, que si k est un diviseur commun de λ et μ et, par suite, un diviseur $k = d$ de leur p.g.c.d. Δ. S'il en est ainsi, le terme en $x^\lambda y^\mu$, en provenance de (3), sera

$$a_d \chi\left(\frac{\lambda}{d}\right) \chi\left(\frac{\mu}{d}\right) x^\lambda y^\mu.$$

Posons $\lambda = \Delta\lambda'$, $\mu = \Delta\mu'$, de sorte que $(\lambda', \mu') = 1$, on voit que le terme en

$$x^\lambda y^\mu = (x^\Delta)^{\lambda'} (y^\Delta)^{\mu'},$$

au second membre de (2) sera

$$\sum_{d \mid \Delta} a_d \chi\left(\frac{\lambda}{d}\right) \chi\left(\frac{\mu}{d}\right) (x^\Delta)^{\lambda'} (y^\Delta)^{\mu'}$$

ou encore, puisque $\chi(n)$ est complètement multiplicative,

$$\left[\sum_{d \mid \Delta} a_d \chi^2\left(\frac{\Delta}{d}\right)\right] \chi(\lambda'\mu') (x^\Delta)^{\lambda'} (y^\Delta)^{\mu'}.$$

Soit donc

$$\gamma(x, y) = \sum_{(l, m)=1} \chi(l\, m) x^l y^m \tag{4}$$

où $l = 1, 2, 3, \ldots$, $m = 1, 2, 3 \ldots$ mais sont premiers entre eux, le p.g.c.d. Δ peut prendre toutes les valeurs entières $1, 2, 3 \ldots$ et, par conséquent, en remarquant que $\chi(1) = 1$

$$G(x, y) = a_1 \gamma(x, y) + \ldots + \left(\sum_{d \mid n} a_d \chi^2\left(\frac{n}{d}\right)\right) \gamma(x^n, y^n) + \ldots. \tag{5}$$

Considérons ensuite la série

$$G(x, y, z) = \sum_{k=1}^{\infty} a_k A(x^k) A(y^k) A(z^k). \tag{6}$$

En raisonnant comme plus haut, cherchons le terme en $x^\lambda y^\mu z^\nu$ au second membre de (6). Désignons par Δ le p.g.c.d. de λ, μ, ν et posons $\lambda = \Delta\lambda'$, $\mu = \Delta\mu'$, $\nu = \Delta\nu'$; λ', μ', ν' seront premiers entre eux dans leur ensemble et le terme cherché en

$$x^\lambda y^\mu z^\nu = (x^\Delta)^{\lambda'}(y^\Delta)^{\mu'}(z^\Delta)^{\nu'}$$

sera

$$\left(\sum_{d|\Delta} a_d \chi^3\left(\frac{\Delta}{d}\right)\right)\chi(\lambda'\mu'\nu')(x^\Delta)^{\lambda'}(y^\Delta)^{\mu'}(z^\Delta)^{\nu'}.$$

Soit alors

$$\gamma(x, y, z) = \sum_{(l,m,n)=1} \chi(lmn) x^l y^m z^n, \tag{7}$$

où les entiers l, m, n varient chacun de 1 à ∞ mais sont premiers entre eux dans leur ensemble, on aura

$$G(x, y, z) = a_1\gamma(x, y, z) + \ldots + \left(\sum_{d|n} a_d \chi^3\left(\frac{n}{d}\right)\right)\gamma(x^n, y^n, z^n) + \ldots. \tag{8}$$

Il est clair que des formules analogues aux précédentes ont lieu quel que soit le nombre des variables qui figurent dans les fonctions G et γ.

2. Series de Dirichlet. Utilisons, comme beaucoup d'auteurs l'ont fait, la correspondance entre

$$x^n \text{ et } n^{-s},\ y^n \text{ et } n^{-s'},\ z^n \text{ et } n^{-s''};$$

l'analogue de $A(x)$ est

$$\mathrm{X}(s) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}, \tag{9}$$

l'analogue de $A(x^k)$ est $k^{-s}\,\mathrm{X}(s)$ et l'analogue de $G(x, y)$ est

$$\sum_{k=1}^{\infty} a_k \frac{\mathrm{X}(s)}{k^s}\frac{\mathrm{X}(s')}{k^{s'}} = \mathrm{X}(s)\mathrm{X}(s')\sum_{k=1}^{\infty}\frac{a_k}{k^{s+s'}}. \tag{10}$$

Posons de plus

$$\mathrm{X}_q(s) = \sum_{n=1}^{\infty} \frac{\chi^q(n)}{n^s}, \qquad q = 2, 3 \ldots \tag{11}$$

et soit, d'autre part, $\xi(s, s')$ l'analogue de $\gamma(x, y)$

$$\xi(s, s') = \sum_{(l,m)=1} \frac{\chi(lm)}{l^s m^{s'}}; \tag{12}$$

l'analogue de $\gamma(x^n, y^n)$ sera $n^{-s-s'}\xi(s, s')$ et le second membre de l'égaligé (5) devient

$$\xi(s, s')\left[\frac{a_1}{1^{s+s'}} + \ldots + \frac{1}{n^{s+s'}}\sum_{d|n} a_d \chi^2\left(\frac{n}{d}\right) + \ldots\right].$$

Le crochet est le produit de

$$\sum_{n=1}^{\infty} \frac{\chi^2(n)}{n^{s+s'}} = X_2(s+s') \quad \text{par} \quad \sum_{n=1}^{\infty} \frac{a_n}{n^{s+s'}};$$

en comparant à (10), on obtient la formule

$$\xi(s, s') = \frac{X(s)X(s')}{X_2(s+s')} \tag{13}$$

Un procédé entièrement semblable donnera, en s'appuyant sur les formules (7) et (8) et en posant

$$\xi(s, s', s'') = \sum_{(l,m,n)=1} \frac{\chi(lmn)}{l^s m^{s'} n^{s''}}, \tag{14}$$

la relation

$$\xi(s, s', s'') = \frac{X(s)X(s')X(s'')}{X_3(s+s'+s'')}. \tag{15}$$

Les formules (13) et (15) sont faciles à démontrer directement. Considérons, par exemple, la formule (14); multiplions les deux membres par

$$\chi^2(k)k^{-s-s'-s''},$$

nous aurons:

$$\frac{\chi^2(k)}{k^{s+s'+s''}} \xi(s, s', s'') = \sum_{(l,m,n)=1} \frac{\chi(lk)\chi(mk)\chi(nk)}{(lk)^s (mk)^{s'} (nk)^{s''}}$$

$$= \sum_{(l,m,n)=k} \frac{\chi(lmn)}{l^s m^{s'} n^{s''}},$$

où k est le p.g.c.d. des trois nombres l, m, et n. Comme les groupes de trois nombres entiers positifs quelconques ont pour p.g.c.d. soit 1, soit 2, soit 3, . . . , on aura, en faisant dans l'égalité précédente $k = 1, 2, 3 \ldots$ et en sommant,

$$X_3(s+s'+s'')\,\xi(s, s', s'') = \sum_{l=1}^{\infty} \frac{\chi(l)}{l^s} \sum_{m=1}^{\infty} \frac{\chi(m)}{m^{s'}} \sum_{n=1}^{\infty} \frac{\chi(n)}{n^{s''}}$$

$$= X(s)X(s')X(s''),$$

ce qui est la formule (15). On peut trouver plusieurs autres démonstrations, notamment en se servant de la décomposition de $X(s)$ en facteurs. Nous allons maintenant donner deux exemples très simples.

3. Exemples. Comme premier exemple, soit $\chi(n)$ un caractère complexe (7, pp. 391–414) au sens de Dirichlet, pour le module 9. Le nombre 9 a deux racines primitives 2 et 5 et $\phi(9) = 6$. Choisissons la racine primitive 2 comme base des indices et $\omega = j = \exp(2\pi i/3)$ comme racine de $x^6 - 1 = 0$. Alors

$$\chi(n) = \omega^{\text{ind}\,n} \text{ et } \chi(n) = 0, \text{ si } 3|n.$$

$$\chi(1) = 1, \quad \chi(2) = j, \quad \chi(3) = 0, \quad \chi(4) = j^2,$$
$$\chi(5) = j^2, \quad \chi(6) = 0, \quad \chi(7) = j, \quad \chi(8) = 1$$
$$\chi(9) = 0$$
$$\chi(n+9) = \chi(n).$$

En conservant les notations de la § 2, on a

$$\xi(s, s') = \frac{X(s)X(s')}{X_2(s+s')}$$

$$\xi(s, s', s'') = \frac{X(s)X(s')X(s'')}{X_3(s+s'+s'')}$$

$$= \frac{X(s)X(s')X(s'')}{(1-3^{-s-s'-s''})\zeta(s+s'+s'')}.$$

$\zeta(\sigma)$ étant la fonction de Riemann. Enfin, comme $\chi^4(n) = \chi(n)$, d'où $X_4(s) = X(s)$, si l'on pose

$$\xi(s_1, s_2 \ldots s_4) = \sum_{(l_1, l_2, \ldots l_4)=1} \frac{\chi(l_1 l_2 \ldots l_4)}{l_1^{s_1} l_2^{s_2} \ldots l_4^{s_4}}$$

on aura

$$\xi(s_1, s_2, s_3, s_4) = \frac{X(s_1)X(s_2)X(s_3)X(s_4)}{X(s_1+s_2+s_3+s_4)}.$$

Si, au lieu de former les caractères (mod 9) avec la racine $\omega = +j$, nous avions choisi la racine $\omega = -j$, il aurait fallu 7 variables $s_1, s_2 \ldots s_7$ pour obtenir

$$\xi(s_1, s_2, \ldots, s_7) = \frac{X(s_1)X(s_2)\ldots X(s_7)}{X(s_1+s_2+\ldots+s_7)}.$$

4. Comme deuxième exemple de fonction complètement multiplicative, nous choisirons la fonction $\lambda(n)$ ainsi définie (**6**, p. 254):

$$n = p_1^{a_1}.p_2^{a_2}\ldots, \qquad \lambda(n) = (-1)^{a_1+a_2+\ldots}.$$

On sait que

$$X(s) = \sum_{n=1}^{\infty} \frac{\lambda(n)}{n^s} = \frac{\zeta(2s)}{\zeta(s)}$$

et il est clair que

$$X_2(s) = \zeta(s).$$

Nous avons donc, d'après le §2, les formules

$$\sum_{(l,m)=1} \frac{\lambda(lm)}{l^s m^{s'}} = \frac{\zeta(2s)\zeta(2s')}{\zeta(s)\zeta(s')\zeta(s+s')}.$$

et

$$\sum_{(l,m,n)=1} \frac{\lambda(lmn)}{l^s m^{s'} n^{s''}} = \frac{\zeta(2s)\zeta(2s')\zeta(2s'')\zeta(s+s'+s'')}{\zeta(s)\zeta(s')\zeta(s'')\zeta(2s+2s'+2s'')}$$

On aurait un exemple analogue en prenant, au lieu de $\lambda(n)$, la fonction $\lambda(n)$ $(-1/n) = \lambda(n) \sin(\frac{1}{2}n\pi)$, utilisée par Landau **(8)**.

5. Symbole de Jacobi. Nous allons maintenant nous borner aux fonctions complètement multiplicatives qui sont les caractères de Dirichlet réels c'est-à-dire égaux à ± 1. On sait qu'un tel caractère se réduit au symbole de Jacobi (D/n).

Pour simplifier, nous supposerons que le nombre D est positif et qu'il n'a pas de diviseur carré. Par suite, si P désigne un produit de facteurs premiers impairs, tous différents, on aura soit $D = P$, soit $D = 2P$. Cela étant nous croyons utile de rassembler, ici quelques propriétés du caractère $\chi(n) = (D/n)$.

$\chi(n)$ est nul, si n n'est pas premier à $2D$. La plus petite période 2ω de $\chi(n)$ est:

$$\text{si } D = P \equiv 1 \pmod 4, \qquad 2\omega = 2P,$$
$$\text{si } D = P \equiv 3 \pmod 4, \qquad 2\omega = 4P,$$
$$\text{si } D = 2P, \qquad 2\omega = 8P,$$

$$\chi(n + 2\omega) = \chi(n). \tag{16}$$

En outre

$$\chi(2\omega - n) = \chi(n), \tag{17}$$

$$\sum_{n=1}^{\omega} \chi(n) = 0, \tag{18}$$

$$\sum_{n=1}^{2\omega} \chi(n) = 0. \tag{19}$$

Les équations (16) à (19) sont valables dans les trois cas.
Quand la période 2ω est divisible par 4 ou par 8, on a

$$\chi(n + \omega) = -\chi(n), \tag{20}$$

mais il n'en est plus de même quand 2ω est le double d'un impair:
Si $2\omega = 4P$, on a

$$\sum_{1}^{\omega} \chi(4k+1) = 0, \qquad \sum_{1}^{\omega} \chi(4k+3) = 0, \tag{21}$$

$$\sum_{1}^{2\omega} \chi(4k+1) = 0, \qquad \sum_{1}^{2\omega} \chi(4k+3) = 0. \tag{22}$$

Enfin, si $2\omega = 8P$, les équations (22) ont lieu, mais non pas les équations (21). Dans les formules ci-dessus, il faut comprendre que l'argument $4.k + 1$, par exemple, prend toutes les valeurs de cette forme plus petites que la limite

supérieure de la somme. Il est clair d'ailleurs que $\chi(n)$ est nul quand n n'est pas premier à 2ω.

6. Polynômes g(x). En gardant les notations de la section précédent, ces polynômes, dont nous avons parlé dans l'Introduction, sont définis par

$$g(x) = \sum_{(\mu, 2\omega)=1} \chi(\mu) x^{\mu}, \qquad \mu < 2\omega \tag{23}$$

Soir $\rho = \exp(\pi i/\omega)$, alors il est visible que, si α est premier à 2ω,

$$g(\rho^{\alpha}) = \chi(\alpha) g(\rho).$$

De plus et c'est la proposition A: *Si la période 2ω est divisible par 4 ou par 8, $g(x)$ admet toutes les racines non primitives de l'équation $x^{2\omega} - 1 = 0$.* Par exemple,

$$\text{si } \chi(n) = \left(\frac{15}{n}\right), \qquad 2\omega = 60,$$

$$g(x) = x + x^{7} + x^{11} - x^{13} + x^{17} - x^{19} - x^{23} - x^{29} - x^{31} - x^{37} - x^{41} + x^{43} - x^{47} + x^{49} + x^{53} + x^{59}$$

$$= x(1 - x^{30})(1 + x^{6})(1 + x^{10})(1 - x^{12})$$

et l,équation aux racines non primitives de $x^{60} - 1 = 0$ est

$$\Phi(x) = \frac{(x^{30} - 1)(x^{10} + 1)(x^{6} + 1)}{x^{2} + 1}.$$

Une telle propriété ne peut plus avoir lieu quand la période 2ω est le double d'un impair. On a en effet, α étant premier à 2ω,

$$\rho^{\alpha+\omega} = -\rho^{\alpha}$$

et

$$g(\rho^{\alpha+\omega}) = -\chi(\alpha) g(\rho).$$

$\alpha + \omega$ est un nombre pair, premier à ω, et $-\rho^{\alpha}$ est une racine primitive de $x^{\omega} - 1 = 0$. Nous avons alors la proposition *B*:

Si 2ω est le double d'un impair, $g(x)$ admet toutes les racines non primitives de $x^{2\omega} - 1 = 0$, sauf celles qui sont racines primitives de $x^{\omega} - 1 = 0$. Par exemple, si

$$\chi(n) = \left(\frac{21}{n}\right), \qquad 2\omega = 42$$

$$g(x) = x + x^{5} - x^{11} - x^{13} + x^{17} - x^{19} - x^{23} + x^{25} - x^{29} - x^{31} + x^{37} + x^{41}$$

$$= x(x^{6} - 1)(x^{14} - 1)(1 + x^{4} + x^{8} + x^{14} + x^{16} + x^{20}).$$

L'équation aux racines non primitives de $x^{42} - 1 = 0$ est

$$\Phi(x) = \frac{(x^{21} - 1)(x^{7} + 1)(x^{3} + 1)}{x + 1} = 0.$$

L'équation aux racines primitives de $x^{21} - 1 = 0$ est

$$F(x) = \frac{(x^{21} - 1)(x - 1)}{(x^3 - 1)(x^7 - 1)} = 0$$

et l'on a

$$\frac{\Phi(x)}{F(x)} = \frac{(x^{14} - 1)(x^6 - 1)}{x^2 - 1}$$

de sorte que

$$g(x) = \frac{\Phi(x)}{F(x)} g_1(x),$$

$g(x_1)$ étant un polynôme.

En vertu de ces deux propositions et en se rappelant que $\chi(m)$ est nul lorsque $(m, 2\omega) > 1$, on voit que si 2ω est divisible par 4 ou par 8,

$$g\left(\exp\left(\frac{2\pi i m}{2\omega}\right)\right) = \chi(m)\, g\left(\exp\left(\frac{2\pi i}{2\omega}\right)\right) \tag{24}$$

quel que soit l'entier m et si 2ω est le double d'un impair, l'équation (24) a encore lieu, sauf pour les $\phi(2\omega)$ valeurs paires de m qui sont premières à ω. Pour ces valeurs $m = \alpha + \omega$, où $(\alpha, 2\omega) = 1$, on a

$$g\left(\exp\left(\frac{2\pi i}{2\omega}(\alpha + \omega)\right)\right) = -\chi(\alpha)\, g\left(\exp\left(\frac{2\pi i}{2\omega}\right)\right). \tag{25}$$

Nous ignorons si ces deux propositions A et B ont été énoncées explicitement. Comme nous l'avons dit en commençant, elles résultent des calculs de Dirichlet **(2)**. Il en est de même, quoique moins facilement, des propriétés multiplicatives qui suivent. Aussi indiquerons-nous très succintement les relations entre caractères qui permettent de les établir.

7. Propriétés multiplicatives de $g\left(\exp\left(\frac{2\pi i m}{2\omega}\right)\right)$.

Rappelons d'abord que, pour les sommes de Ramanujan

$$c_q(m) = \sum_{(\mu, q)=1} \exp\left(\frac{2\pi i \mu m}{q}\right) \tag{26}$$

on a, lorsque $(q, q') = 1$,

$$c_q(m) c_{q'}(m) = c_{qq'}(m).$$

Les propriétés que nous allons énoncer comportent cinq cas différents. Posons

$$\chi(n) = \left(\frac{D}{n}\right), \qquad \chi'(n) = \left(\frac{D'}{n}\right),$$

$$\chi_1(n) = \left(\frac{DD'}{n}\right);$$

soient 2ω, $2\omega'$ et $2\omega_1$ les plus petites périodes respectives de $\chi(n)$, $\chi'(n)$ et $\chi_1(n)$.

h, h', h_1 désignant respectivement les entiers premiers à 2ω, $2\omega'$, $2\omega_1$ et $< 2\omega$, $2\omega'$, $2\omega_1$, nous poserons

$$g(x) = \sum \chi(h)x^h, \qquad g'(x) = \sum \chi'(h')x^{h'},$$

$$g_1(x) = \sum \chi_1(h_1)x^{h_1};$$

nous poserons encore

$$\rho = \exp\left(\frac{2\pi i}{2\omega}\right), \qquad \rho' = \exp\left(\frac{2\pi i}{2\omega'}\right), \qquad \rho_1 = \exp\left(\frac{2\pi i}{2\omega_1}\right).$$

Enfin P et P' seront deux entiers positifs impairs, premiers entre eux, et m est un entier positif quelconque.

1er Cas:

$$D = 2P, \qquad D' = P' \equiv 3 \pmod 4$$

$$g(\rho^m)g'(\rho'^m) = 2g_1(\rho_1{}^m).$$

La démonstration repose sur

$$\left(\frac{2PP'}{P'h + 2Ph'}\right) = \left(\frac{2P}{h}\right)\left(\frac{P'}{h'}\right).$$

2^{ième} Cas: $D = 2P$, $D' = P' \equiv 1 \pmod 4$

$$g(\rho^m)g'(\rho'^m) = -\left(\frac{2}{P'}\right)g_1(\rho_1^m).$$

La démonstration repose sur

$$\left(\frac{2PP'}{P'h + 4Ph'}\right) = -\left(\frac{2}{P'}\right)\left(\frac{2P}{h}\right)\left(\frac{P'}{h'}\right).$$

3^{ième} Cas: $D = P \equiv 1 \pmod 4$, $D' = P' \equiv 3 \pmod 4$

$$g(\rho^m)g'(\rho'^m) = -\left(\frac{2}{P}\right)g_1(\rho_1^m).$$

La démonstration repose sur

$$\left(\frac{PP'}{Ph' + 2P'h}\right) = -\left(\frac{2}{P}\right)\left(\frac{P}{h}\right)\left(\frac{P'}{h'}\right)$$

4^{ième} Cas: $D = P \equiv 1 \pmod 4$, $D' = P' \equiv 1 \pmod 4$.

$$g(\rho^m)g'(\rho'^m) = e^{m\pi i}g_1(\rho_1^m).$$

La démonstration repose sur ce que, si

$$h_1 = Ph' + P'h + PP',$$

on a

$$\left(\frac{PP'}{h_1}\right) = \left(\frac{P}{h}\right)\left(\frac{P'}{h'}\right).$$

5ième Cas: $D = P \equiv 3 \pmod 4$, $D' = P' \equiv 3 \pmod 4$

$$g(\rho^m)g'(\rho'^m) = -\left(\frac{2}{PP'}\right) 2(1 - \varepsilon^{m\pi i}) g_1(\rho_1^m).$$

La démonstration repose sur ce que: d'une part, si $h_1 = (P'h + Ph')/2$ est impair,

$$\left(\frac{PP'}{h_1}\right) = -\left(\frac{2}{PP'}\right)\left(\frac{P}{h}\right)\left(\frac{P'}{h'}\right),$$

d'autre part, si $h_1 = (P'h + Ph')/2$ est pair,

$$\left(\frac{PP'}{h_1 + PP'}\right) = \left(\frac{2}{PP'}\right)\left(\frac{P}{h}\right)\left(\frac{P'}{h'}\right).$$

8. Il résulte, en définitive, des équations (24) et (25) que la connaissance de $g\,(\exp(\pi im/\omega))$ est ramenée à celle de $g\,(\exp(\pi i/\omega))$. Celle-ci exige la connaissance des sommes de Gauss. Les calculs de Dirichlet **(2**, pp. 188–93**)** montrent que si

$$\chi(n) = \left(\frac{P}{n}\right), \qquad P \equiv 1 \pmod 4;\ 2.\omega = 2P,$$

$$g\left(\exp\left(\frac{2\pi i}{2P}\right)\right) = -\left(\frac{2}{P}\right)\sqrt{P};$$

si

$$\chi(n) = \left(\frac{P}{n}\right), \qquad P \equiv 3 \pmod 4, \qquad 2\,.\,\omega = 4P,$$

$$g\left(\exp\left(\frac{2\pi i}{4P}\right)\right) = \sqrt{4P};$$

si

$$\chi(n) = \left(\frac{2P}{n}\right), \qquad 2\omega = 8P,$$

$$g\left(\exp\left(\frac{2\pi i}{8P}\right)\right) = \sqrt{8P}.$$

9. Nous revenons à la série (1) du §1, en supposant que $\chi(n)$ est le symbole de Jacobi du § 5, ayant la période 2ω. On a alors

$$A(x) = \frac{g(x)}{1 - x^{2\omega}},$$

où $g(x)$ est le polynôme (23). La série (2) devient

$$G(x, y) = \sum_{k=1}^{\infty} a_k \frac{g(x^k)}{1 - x^{2.\omega.k}} \frac{g(y^k)}{1 - y^{2\omega k}} \tag{27}$$

et la formule (5) subsiste. Cherchons quel est, au second membre de (4), le coefficient de $\chi(m)y^m$, sans nous inquiéter de la valeur, nulle ou non nulle, de $\chi(m)$. Ce sera

$$\sum_{(l,m)=1} \chi(l)x^l.$$

Comme $\chi(l)$ a la période 2ω et que l doit être premier à m, on aura

$$\sum_{(l,m)=1} \chi(l)x^l = \frac{f(x, 2m\omega)}{1 - x^{2m\omega}}$$

où

$$f(x, 2m\omega) = \sum_{(\mu,m)=1} \chi(\mu)x^{\mu}, \tag{28}$$

$$1 \leqslant \mu \leqslant 2m \,.\, \omega - 1$$

ou bien, si l'on veut, d'après les propriétés de $\chi(\mu)$,

$$f(x, 2m\omega) = \sum_{(\mu,\, 2m\omega)=1} \chi(\mu)x^{\mu}, \tag{29}$$

$$1 \leqslant \mu \leqslant 2m \,.\, \omega - 1.$$

On voit que $g(x) = f(x, 2\omega)$. Ainsi

$$\gamma(x, y) = \sum_{q=1}^{\infty} \chi(q)y^q \frac{f(x, 2q\omega)}{1 - x^{2q\omega}}. \tag{30}$$

On obtient une autre expression du polynôme $f(x, 2q\omega)$ de la manière suivante. Identifions les termes en a_1 au second membre de (27) et au second membre de (5), nous obtenons

$$\frac{g(x)}{1 - x^{2\omega}} \frac{g(y)}{1 - y^{2\omega}} = \sum_{n=1}^{\infty} \chi^2(n)\gamma(x^n, y^n). \tag{31}$$

L'inversion de cette formule est facile; elle revient, comme on le sait, ayant

$$G(s) = F(s) \sum_{n=1}^{\infty} \frac{\chi^2(n)}{n^s}$$

à en déduire

$$F(s) = G(s) \sum_{n=1}^{\infty} \mu(n) \frac{\chi^2(n)}{n^s},$$

où $\mu(n)$ est la fonction de Möbius. On a donc

$$\gamma(x, y) = \sum_{k=1}^{\infty} \mu(k)\, \chi^2(k) \frac{g(x^k)}{1 - x^{2\omega k}} \frac{g(y^k)}{1 - y^{2\omega k}} \tag{32}$$

Le terme en y^q, au second membre de (32), est

$$y^q \sum_{d|q} \mu(d) \chi^2(d) \chi\left(\frac{q}{d}\right) \frac{g(x^d)}{1 - x^{2\omega d}}$$

et, en comparant à (30), on trouve

$$\chi(q) f(x, 2q\omega) = \sum_{d|q} \mu(d) \chi^2(d) \chi\left(\frac{q}{d}\right) g(x^d) \frac{1 - x^{2q\omega}}{1 - x^{2d\omega}} \tag{33}$$

et, comme

$$\chi^2(d) \chi\left(\frac{q}{d}\right) = \chi(q) \cdot \chi(d),$$

on a aussi, en divisant les deux membres par $\chi(q)$,

$$f(x, 2q\omega) = \sum_{d|q} \mu(d) \chi(d) g(x^d) \frac{1 - x^{2q\omega}}{1 - x^{2d\omega}}. \tag{34}$$

Cette formule (34) subsiste même si $\chi(q)$ est nul car si l'on pose, pour un instant

$$h(x) = g(x) \frac{1 - x^{2q\omega}}{1 - x^{2\omega}},$$

le second membre de (34) n'est autre que le polynôme $h(x)$, privé des termes $\chi(\mu)x^{\mu}$, où μ n'est pas premier à q. C'est donc bien le polynôme $f(x, 2q\omega)$.

10. Séries analogues à une série de Ramanujan. Nous allons chercher une expression de la somme des trois séries

$$S = \sum_{q=1}^{\infty} f(x^{n|q}, 2q\omega) \frac{1}{q^s},$$

$$S_1 = \sum_{q=1}^{\infty} f(x^{n|q}, 2q\omega) \frac{\chi(q)}{q^s},$$

$$S_2 = \sum_{q=1}^{\infty} f(x^{n|q}, 2q\omega) \frac{\chi^2(q)}{q^s},$$

où n désigne un entier positif quelconque et en nous bornant, pour simplifier, aux cas où la période 2ω de $\chi(n)$ est divisible par 4 ou par 8. Dans ces cas, a lieu la formule (24). En outre $X(s)$ et $X_2(s)$ auront les significations (9) et (11) du § 2.

Dans la formule (34), remplaçons x par $x^{n/q}$; elle devient

$$(35) \qquad f(x^{n/q}, 2q\omega) = \sum_{d|q} \mu\left(\frac{q}{d}\right)\chi\left(\frac{q}{d}\right) g(x^{n/d}) \frac{1 - x^{2n\omega}}{1 - x^{2n\omega/d}}$$

et, en substituant cette expression dans S, on voit que le second membre est le produit de

$$\sum_{q=1}^{\infty} \frac{\mu(q) \cdot \chi(q)}{q^s}$$

par

$$\sum_{q=1}^{\infty} g(x^{n/q}) \frac{1 - x^{2n\omega}}{1 - x^{2n\omega/q}} \frac{1}{q^s}.$$

On a donc

$$(36) \qquad S = \frac{1}{\mathrm{X}(s)} \sum_{q=1}^{\infty} g(x^{n/q}) \frac{1 - x^{2n\omega}}{1 - x^{2n\omega/q}} \cdot \frac{1}{q^s}.$$

De même, en remplaçant x par $x^{n/q}$, dans la formule (33), et en substituant dans S_1, nous aurons

$$(37) \qquad S_1 = \frac{1}{\mathrm{X}_2(s)} \sum_{q=1}^{\infty} \chi(q) g(x^{n/q}) \frac{1 - x^{2n\omega}}{1 - x^{2n\omega/q}} \cdot \frac{1}{q^s}.$$

Enfin, on déduit de (35)

$$\chi^2(q) f(x^{n/q}, 2q\omega) = \sum_{d|q} \mu\left(\frac{q}{d}\right)\chi\left(\frac{q}{d}\right)\chi^2(d) g(x^{n/d}) \frac{1 - x^{2n\omega}}{1 - x^{2n\omega/d}}$$

et, en substituant dans S_2, on obtient

$$(38) \qquad S_2 = \frac{1}{\mathrm{X}(s)} \sum_{q=1}^{\infty} \chi^2(q) g(x^{n/q}) \frac{1 - x^{2n\omega}}{1 - x^{2n\omega/q}} \cdot \frac{1}{q^s}.$$

Faisons maintenant $x = \exp(2\pi i/2\omega)$ dans les trois équations (36), (37), et (38);
le facteur

$$\frac{1 - x^{2n\omega}}{1 - x^{2n\omega/q}}$$

est nul si q ne divise pas n et est égal à q si q divise n. Nous avons donc

$$(39) \qquad \sum_{q=1}^{\infty} f\left(\exp\left(\frac{2\pi i n}{2q\omega}\right), 2q\omega\right) \frac{1}{q^s} = \frac{g\left(\exp\left(\frac{2\pi i}{2\omega}\right)\right)}{n^{s-1}\mathrm{X}(s)} \sum_{d|n} \chi(d) d^{s-1},$$

$$(40) \qquad \sum_{q=1}^{\infty} f\left(\exp\left(\frac{2\pi i n}{2q\omega}\right), 2q\omega\right) \frac{\chi(q)}{q^s} = \frac{\chi(n)\, g\left(\exp\left(\frac{2\pi i}{2\omega}\right)\right)}{n^{s-1}\mathrm{X}_2(s)} \sum_{d|n} d^{s-1},$$

$$(41) \qquad \sum_{q=1}^{\infty} f\left(\exp\left(\frac{2\pi i n}{2q\omega}\right), 2q\omega\right) \frac{\chi^2(q)}{q^s} = \frac{\chi(n)\, g\left(\exp\left(\frac{2\pi i}{2\omega}\right)\right)}{n^{s-1}\mathrm{X}(s)} \sum_{d|n} \chi\left(\frac{n}{d}\right) d^{s-1}.$$

Ce sont ces trois dernières formules que l'on peut considérer comme étant analogues à la formule de Ramanujan **(6**, pp. 55, 237**)**

$$\sum_{q=1}^{\infty} \frac{c_q(n)}{q^s} = \frac{1}{n^{s-1}\zeta(s)} \sum_{d|n} d^{s-1}.$$

Si nous supposons l'entier n premier à 2ω, ses diviseurs d le sont aussi et $\chi(n/d) = \chi(n)\chi(d)$, de sorte que les seconds membres de (39) et (41) sont les mêmes et, par suite, les premiers membres sont égaux. C'est ce que l'on peut démontrer directement. Il faut observer que, lorsque n.q est premier à 2ω, la somme

$$f\left(\exp\left(\frac{2\pi i n}{2q\omega}\right), 2q\omega\right)$$

a un rapport étroit avec la somme de Ramanujan (26), dont l'expression arithmétique est **(6**, p. 237**)**

$$c_q(n) = \sum_{d|q.d|n} \mu\left(\frac{q}{d}\right) d. \tag{42}$$

Reprenons en effet la formule (35) et faisons

$$x = \exp\left(\frac{2\pi i}{2\omega}\right),$$

nous obtenons

$$f\left(\exp\left(\frac{2\pi i n}{2q\omega}\right), 2q\omega\right) = g\left(\exp\left(\frac{2\pi i}{2\omega}\right)\right) \sum_{d|q.d|n} \mu\left(\frac{q}{d}\right)\chi\left(\frac{q}{d}\right)\chi\left(\frac{n}{d}\right) . d.$$

Or

$$\chi\left(\frac{q}{d}\right)\chi\left(\frac{n}{d}\right) = \frac{\chi(qn)}{\chi^2(d)} = \chi(qn), \tag{43}$$

car $\chi(d)$ n'est pas nul, donc

$$\begin{aligned} f\left(\exp\left(\frac{2\pi i n}{2q\omega}\right), 2q\omega\right) &= g\left(\exp\left(\frac{2\pi i}{2\omega}\right)\right) \chi(q\,.\,n) \sum_{d|q.d|n} \mu\left(\frac{q}{d}\right) . d \\ &= g\left(\exp\left(\frac{2\pi i}{2\omega}\right)\right) \chi(q\,.\,n)\, c_q(n). \end{aligned} \tag{44}$$

La formule (44) subsisterait si un seul des nombres q et n avait un diviseur commun avec 2ω, mais son second membre serait nul. Si, au contraire, q et n avaient chacun un diviseur commun avec 2ω, la formule (44) n'aurait plus lieu.

11. Exemple. Prenons

$$\chi(n) = \left(\frac{-1}{n}\right);$$

Ici, $D = -1$ est négatif, ce que nous avions exclu précédemment, notamment de la § 8, mais on a facilement

$$X(s) = 1 - \frac{1}{3^s} + \frac{1}{5^s} - \frac{1}{7^s} + \ldots = L(s),$$

(45)

$$X_2(s) = 1 + \frac{1}{3^s} + \frac{1}{5^s} + \frac{1}{7^s} + \ldots = (1 - 2^{-s})\,\zeta(s)$$

la période de $\chi(n)$ est $2\omega = 4$

$$g(x) = x - x^3,\ g\left(\exp\left(\frac{2\pi i}{4}\right)\right) = 2i,\ g\left(\exp\left(\frac{2\pi i m}{4}\right)\right) = 2i\,.\,\chi(m)$$

$$f(x, 4q) = \sum_{(\mu, 4q)=1} \chi(\mu) x^{\mu}, \qquad \mu < 4q$$

et l'application des formules (39) à (41) nous donne

$$(46)\quad \sum_{q=1}^{\infty} f\left(\exp\left(\frac{2\pi i n}{4q}\right), 4q\right) \frac{1}{q^s} = \frac{2i}{n^{s-1} L(s)} \sum_{d \mid n} \chi(d)\, d^{s-1}$$

$$\sum_{q=1}^{\infty} f\left(\exp\left(\frac{2\pi i n}{4q}\right), 4q\right) \frac{\chi(q)}{q^s} = \frac{2i\chi(n)}{(1 - 2^{-s})\zeta(s)} \frac{\sigma_{s-1}(n)}{n^{s-1}}$$

$$\sum_{q=1}^{\infty} f\left(\exp\left(\frac{2\pi i n}{4q}\right), 4q\right) \frac{\chi^2(q)}{q^s} = \frac{2i\chi(n)}{n^{s-1} L(s)} \sum_{d \mid n} \chi\left(\frac{n}{d}\right) d^{s-1}.$$

On voit sur (46) que, si les facteurs premiers impairs de n sont tous $\equiv 1 \pmod 4$, il en est de même pour tous les diviseurs impairs de n et, dans ce cas, le second membre de (46) se réduit à

$$\frac{2i\sigma_{s-1}(n)}{n^{s-1} L(s)}.$$

Enfin, d'après (44), si $n\,q$ est impair,

$$f\left(\exp\left(\frac{2\pi i n}{4q}\right), 4q\right) = 2i\ \chi(n\,.\,q) c_q(n).$$

12. Nous signalons qu'on peut obtenir une généralisation des résultats des §§ 9 et 10 en partant de la formule (7) que nous récrivons

$$\gamma(x, y, z) = \sum_{(l, m, n)=1} \chi(l)\chi(m)\chi(n) x^l y^m z^n$$

et de l'équation (8) dont on tirera, comme tout à l'heure, par inversion

$$(47)\qquad \gamma(x, y, z) = \sum_{k=1}^{\infty} \mu(k)\chi(k) \frac{g(x^k)}{1 - x^{2\omega k}} \frac{g(y^k)}{1 - y^{2\omega k}} \frac{g(z^k)}{1 - z^{2\omega k}}.$$

La formule (47) se prête au développement du premier membre suivant les puissances d'une des variables, z par exemple, et la formule (7) se prête au

développement suivant les fonctions $\gamma(x, y)$, $\gamma(x^2, y^2), \ldots, \gamma(x^n, y^n), \ldots$. On peut ainsi trouver des sommes et des séries analogues à celles de Ramanujan.

13. Intégrales définies. Schlömilch **(11**, p. 277**)**, en transformant une intégrale d'Abel, a donné la formule

$$(48) \qquad \int_0^\infty \frac{u^{y-1}du}{(l+mu)^{x+y}} = \frac{\Gamma(x)\,.\,\Gamma(y)}{\Gamma(x+y)}\,\frac{1}{l^x m^y}\,, \qquad R(x)>1, R(y)>1.$$

Posons

$$(49) \qquad P(u,\sigma) = \sum_{(l,m)=1} \frac{1}{(l+mu)^\sigma}\,, R(\sigma)>2,$$

nous aurons

$$(50) \qquad \int_0^\infty u^{s'-1} P(u, s+s')\,du = \frac{\Gamma(s)\Gamma(s')}{\Gamma(s+s')}\,\frac{\zeta(s)\zeta(s')}{\zeta(s+s')}\,.$$

Si nous multiplions les deux membres de (49) par $\zeta(\sigma)$, il viendra

$$(51) \qquad \zeta(\sigma)P(u,\sigma) = Q(u,\sigma) = \sum_{l=1}^{\infty}\ \sum_{m=1}^{\infty} \frac{1}{(l+mu)^\sigma}$$

et par suite,

$$(52) \qquad \int_0^\infty u^{s-1}\,Q(u, s+s')\,du = \frac{\Gamma(s)\,.\,\Gamma(s')}{\Gamma(s+s')}\,\zeta(s)\,.\,\zeta(s')\,.$$

Il semble que la formule (50) puisse présenter un certain intérêt. Lorsque s et s' sont des entiers pairs, l'intégrale du premier membre est un nombre rationnel et on peut rappeler qu'Euler **(5**, p. 350**)** a cherché des expressions, telles que:

$$\zeta(3) = 2^2 B_{3/2}\,\frac{\pi^3}{3!}\,, \qquad B_{3/2} = 0{,}05815227\ldots$$

$$\zeta(5) = 2^4 B_{5/2}\,\frac{\pi^5}{5!}\,, \qquad B_{5/2} = 0{,}02541327\ldots$$

$$\ldots$$

Partons maintenant d'une intégrale qui se déduit aisément d'une formule de Liouville **(3**, p. 150**)**:

$$(53) \qquad \int_0^\infty\int_0^\infty \frac{u^{s'-1}v^{s''-1}dudv}{(l+mu+nv)^{s+s'+s''}} = \frac{\Gamma(s)\Gamma(s')\Gamma(s'')}{\Gamma(s+s'+s'')}\,\frac{1}{l^s m^{s'} n^{s''}}\,,$$

où les parties réelles de s, s', s'' sont > 1, et posons

$$(54) \qquad P(u,v,\sigma) = \sum_{(l,m,n)=1} \frac{1}{(l+mu+nv)^\sigma}\,, \qquad R(\sigma)>3,$$

nous aurons

$$(55) \qquad \int_0^\infty\int_0^\infty u^{s-1}v^{s'-1}P(u,v,s+s'+s'')\,du\,dv$$

$$= \frac{\Gamma(s)\Gamma(s')\Gamma(s'')}{\Gamma(s+s'+s'')}\,.\,\frac{\zeta(s)\zeta(s')\zeta(s'')}{\zeta(s+s'+s'')}\,.$$

Nous poserons encore

$$Q(u, v, \sigma) = \zeta(\sigma)P(u, v, \sigma) \tag{56}$$

$$= \sum_{l=1}^{\infty} \sum_{m=1}^{\infty} \sum_{n=1}^{\infty} \frac{1}{(l + mu + nv)^{\sigma}}$$

et, en multipliant les deux membres de (55) par $\zeta(s + s' + s'')$, nous obtiendrons une nouvelle formule qu'il est inutile d'écrire.

14. En supposant que $\chi(n)$ est un caractère réel et en posant comme au § 2

$$\mathrm{X}(s) = \sum_{n=1}^{\infty} \chi(n)n^{-s}, \qquad \mathrm{X}_2(s) = \sum_{n=1}^{\infty} \chi^2(n)n^{-s},$$

$$\mathrm{X}_3(s) = \mathrm{X}(s)$$

les calculs précédents s'étendent facilement. Soit

$$P(\chi, u, \sigma) = \sum_{(l,m)=1} \frac{\chi(lm)}{(l + mu)^{\sigma}}, \qquad R(\sigma) > 2,$$

$$P(\chi, u, v, \sigma) = \sum_{(l,m,n)=1} \frac{\chi(lmn)}{(l + mu + nv)^{\sigma}}, \qquad R(\sigma) > 3,$$

et soit également

$$\mathrm{X}_2(\sigma)P(\chi, u, \sigma) = Q(\chi, u, \sigma) = \sum_{l=1}^{\infty} \sum_{m=1}^{\infty} \frac{\chi(lm)}{(l + mu)^{\sigma}},$$

$$\mathrm{X}(\sigma)P(\chi, u, v, \sigma) = Q(\chi, u, v, \sigma) = \sum_{l=1}^{\infty} \sum_{m=1}^{\infty} \sum_{n=1}^{\infty} \frac{\chi(lmn)}{(l + mu + nv)^{\sigma}}$$

nous aurons en partant des intégrales (48) et (53)

$$\int_0^{\infty} u^{s-1}P(\chi, u, s + s')\,du = \frac{\Gamma(s)\,.\,\Gamma(s')}{\Gamma(s + s')} \frac{\mathrm{X}(s)\mathrm{X}(s')}{\mathrm{X}_2(s + s')},$$

$$\int_0^{\infty} \int_0^{\infty} u^{s-1}v^{s'-1}P(\chi, u, v, s + s' + s'')\,du\,dv$$

$$= \frac{\Gamma(s)\Gamma(s')\Gamma(s'')}{\Gamma(s + s' + s'')} \frac{\mathrm{X}(s)\mathrm{X}(s')\mathrm{X}(s'')}{\mathrm{X}(s + s' + s'')}$$

$$\int_0^{\infty} u^{s-1}Q(\chi, u, s + s')\,du = \frac{\Gamma(s)\Gamma(s')}{\Gamma(s + s')} \mathrm{X}(s)\mathrm{X}(s'),$$

$$\int_0^{\infty} \int_0^{\infty} u^{s-1}v^{s'-1}Q(\chi, u, v, s + s' + s'')\,du\,dv$$

$$= \frac{\Gamma(s)\,.\,\Gamma(s')\,.\,\Gamma(s'')}{\Gamma(s + s' + s'')} \mathrm{X}(s)\mathrm{X}(s')\mathrm{X}(s'').$$

Prenons en particulier le même caractère $\chi(n)$ que dans la § 11, nous aurons

$$(57) \qquad \int_0^\infty u^{s-1}P(\chi, u, s+s')\,du = \frac{\Gamma(s)\,.\,\Gamma(s')}{\Gamma(s+s')}\,\frac{L(s)L(s')}{(1-2^{-s-s'})\zeta(s+s')}$$

et

$$\int_0^\infty\int_0^\infty u^{s-1}v^{s'-1}P(\chi, u, v, s+s'+s'')\,du\,dv$$

$$= \frac{\Gamma(s)\,.\,\Gamma(s')\,.\,\Gamma(s'')}{\Gamma(s+s'+s'')}\,\frac{L(s)L(s')L(s'')}{L(s+s'+s'')}\,.$$

15. Voici quelques exemples d'application de l'intégrale (50) que nous désignons par I (s, s') et de l'intégrale (57) que nous désignons par $J(s, s')$. On sait **(9**, p. 33**)** que

$$\zeta(2n) = \tfrac{1}{2}(2\pi)^{2n}\cdot\frac{B_n}{(2n)!}$$

$$L(2n+1) = \tfrac{1}{2}\left(\frac{\pi}{2}\right)^{2n+1}\frac{E_n}{(2n)!}$$

$B_1 = 1/6$, $B_2 = 1/30$, . . . sont les nombres de Bernoulli $E_0 = 1$, $E_1 = 1$, $E_2 = 5$, . . ., sont les nombres d'Euler. On trouve leurs valeurs dans **(10**, pp. 176–8**)**

$$I(2,2) = \frac{5}{12} \qquad J(1,3) = \frac{1}{4}$$

$$I(2,4) = \frac{7}{2^4\,.\,5} \qquad J(1,5) = \frac{5}{32}$$

$$I(3,3) = \frac{3^2\,.\,7}{2^5}\,\zeta^2(3) \qquad J(3,3) = \frac{1}{32}$$

$$I(2,6) = \frac{5}{2\,.\,3^2\,.\,7} \qquad J(1,7) = \frac{61}{2^5\,.\,17}$$

$$I(3,5) = \frac{2\,.\,3^2\,.\,5}{\pi^8}\,\zeta(3)\zeta(5) \qquad J(3,5) = \frac{5}{2^5\,.\,17}$$

$$I(5,5) = \frac{3^3\,.\,11}{2\,.\,\pi^{10}}\,\zeta(5) \qquad J(5,5) = \frac{5^2}{2^9\,.\,31}\,.$$

On voit qu'on peut obtenir des relations algébriques entre ces intégrales.

16. Considérons l'intégrale (52). Il n'est pas évident qu'elle a un sens car, pour la fonction $Q(u, \sigma)$, l'axe réel négatif est une ligne de points essentiels, y compris le point $u = 0$, et on voit directement qu'en faisant tendre u vers zéro par valeurs positives, $Q(u, \sigma)$ devient infini. Mais on établit sans peine la formule

$$(58) \qquad \Gamma(\sigma)Q(u, \sigma) = \int_0^\infty \frac{x^{\sigma-1}dx}{(e^x-1)(e^{u\cdot x}-1)}\,. \qquad R(\sigma) > 2.$$

En supposant u très petit positif, on a

$$\frac{1}{e^{ux}-1}=\frac{1}{ux}$$

et

$$\Gamma(\sigma)Q(u,\sigma)=\frac{1}{u}\Gamma(\sigma-1)\zeta(\sigma-1)$$

ou bien

$$Q(u,\sigma)=\frac{\zeta(\sigma-1)}{\sigma-1}\frac{1}{u},$$

et

$$P(u,\sigma)=\frac{1}{\sigma-1}\frac{\zeta(\sigma-1)}{\zeta(\sigma)}\frac{1}{u}.$$

On arriverait au même résultat en faisant, dans (58), u très grand positif et en se servant ensuite de la relation

$$Q\left(\frac{1}{u},\sigma\right)=u^{\sigma}\,.\,Q(u,\sigma).$$

Les intégrales (50) et (52) ont donc bien un sens, puisque $R(s)$ et $R(s')$ sont >1. Si nous considérons l'intégrale (52), en nous servant de (58) pour $\sigma=s+s'$, nous aurons

$$(59)\qquad \int_0^{\infty}u^{s'-1}\,du\int_0^{\infty}\frac{x^{s+s'-1}\,dx}{(e^{x}-1)(e^{ux}-1)}=\Gamma(s)\zeta(s)\Gamma(s')\zeta(s').$$

Posons $u=y/x$ et le premier membre devient

$$\int_0^{\infty}\frac{y^{s'-1}\,dy}{e^{y}-1}\int_0^{\infty}\frac{x^{s-1}\,dx}{e^{x}-1},$$

ce qui constitue une démonstration directe de (59), donc de (52) et, par suite, de (50).

References

1. P. Bachmann, *Zahlentheorie*, Teil 1.
2. ——— *Zahlentheorie*, Teil 2.
3. G. Brunel, *Monographie de la fonction gamma.*
4. E. Cahen, *Théorie des nombres*, T. 2.
5. L. Euler, *Oeuvres*, Series Prima Vol. X.
6. G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers* (2nd ed.; Oxford, 1954).
7. E. Landau, *Primzahlen*, vol. I.
8. ——— *Primzahlen*, vol. II.
9. E. Lindelöf, *Le Calcul des résidus.*
10. N. Nielsen, *Traité élémentaire des nombres de Bernoulli.*
11. O. Schlömilch, *Compendium der Höheren analysis*, vol. II.

Lausanne, Suisse

POWER SERIES REPRESENTING CERTAIN RATIONAL FUNCTIONS

Z. A. MELZAK

1. Let $\mathfrak{A}$ denote the set of functions of a complex variable z, regular at $z = 0$, and let I denote the set of non-negative integers. For $f \in \mathfrak{A}$ put

$$f(z) = \sum_{n=0}^{\infty} f_n z^n, \quad \phi_f(z) = \sum_{n=0}^{\infty} \operatorname{sgn}|f_n| z^n, \quad I_f = \{n | n \in I, f_n = 0\}.$$

For a given subset $\mathfrak{A}_0$ of $\mathfrak{A}$ there arises the problem of characterizing the admissible gap sets I_f of functions f in $\mathfrak{A}_0$. When $\mathfrak{A}_0$ is the set $\mathfrak{R}$ of rational functions a complete solution in given by the following theorem:

(A) *Let $f \in \mathfrak{R}$ and let I_f be infinite. Then there exist integers $L, L_1, L_2, \ldots, L_s$, such that $0 \leqslant L_1 < L_2 \ldots < L_s < L$, and $I_f = \{n | n \in I,\ n \equiv L_j \pmod{L},\ j = 1, \ldots, s\} \cup I'$, where I' is a finite exceptional set.*

As in **(2)**, this is simply deduced from the theorem

(B) *Let $f \in \mathfrak{R}$ and let I_f be infinite. Then there exist integers L, L_1, n_0, such that $0 \leqslant L_1 < L$, $n_0 \geqslant 0$, and $\{n | n_0 \leqslant n,\ n \equiv L_1 \pmod{L}\} \subset I_f$.*

Theorem (A) was proved in 1934 by Mahler for the case when f has algebraic coefficients. This was extended to the general case by Lech in 1953; later, in 1957 Mahler gave another proof of the general case. For references see **(1)** and **(2)**.

We shall prove first

LEMMA 1. *Theorem* (A) *is equivalent to the proposition: if $f \in \mathfrak{R}$ then $\phi_f \in \mathfrak{R}$.*

In view of this one may ask the following question: let

$$f = \sum_{n=0}^{\infty} f_n z^n \in \mathfrak{R}$$

and let the coefficients f_n be all real, put

$$\chi_f(z) = \sum_{n=0}^{\infty} \operatorname{sgn} f_n z^n;$$

under what conditions is $\chi_f \in \mathfrak{R}$? Our main result proves the existence of a large class of such functions f and indicates some of its properties.

2. There are several descriptions of $\mathfrak{R}$ which we shall use. Their well-known equivalence is stated formally as

Received September 18, 1958.

LEMMA 2. *The following are equivalent:*

(a) $\mathfrak{R}$ *is the set of quotients* $P(z)/Q(z)$ *of polynomials with complex coefficients and with* $Q(0) \neq 0$,

(b) $\mathfrak{R}$ *is the set of sums of the form*

$$P(z) + \sum_{k=1}^{N} \sum_{j=1}^{M} A_{jk} (\alpha_k - z)^{-j}$$

where P *is a polynomial,* A_{jk} *and* α_k *are complex constants, and* $\alpha_k \neq 0$,

(c) $\mathfrak{R}$ *is the set of power series*

$$\sum_{n=0}^{\infty} f_n z^n,$$

regular at $z = 0$, *whose coefficients satisfy a linear recurrence relation:*

$$\sum_{j=0}^{N} c_j f_{n+j} = 0, \qquad n > n_0,$$

(d) $\mathfrak{R}$ *is the set of power series*

$$\sum_{n=0}^{\infty} f_n z^n,$$

regular at $z = 0$, *whose coefficients are values of an exponential polynomial:*

$$f_n = \sum_{k=1}^{N} P_k(n) \alpha_k^{-n}, \qquad n > n_0,$$

where P_k *is a polynomial and* $\alpha_k \neq 0$.

Here and in the sequel "$T(n)$, $n > n_0$" will mean that the property T holds for all non-negative integers greater than or equal to n_0. The bound n_0 will vary from case to case.

Let

$$f = \sum_{n=0}^{\infty} f_n z^n \in \mathfrak{R}, g = \sum_{n=0}^{\infty} g_n z^n \in \mathfrak{R},$$

and put

$$f \circ g = \sum_{n=0}^{\infty} f_n g_n z^n. \tag{1}$$

By Hadamard's Multiplication Theorem **(3)**,

$$(f \circ g)(z) = 1/2\pi i \int_C f(w)\, g(z/w)\, dw/w \tag{2}$$

where C is a sufficiently small simple contour about the origin. By Lemma 2, (d), or directly by (2), $f \circ g \in \mathfrak{R}$ if $f, g \in \mathfrak{R}$. It follows that under the ordinary addition and the multiplication of (1) $\mathfrak{R}$ becomes a commutative algebra over the complex numbers, with the identity $e(z) = 1/(1 - z)$.

3. We prove now Lemma 1. Let

$$f = \sum_{n=0}^{\infty} f_n z^n \in \mathfrak{R};$$

without loss of generality let I_f be infinite. By Theorem (A)

$$\phi_f(z) = e(z) - e(z^L)P(z) + Q(z)$$

where P and Q are polynomials and

$$P(z) = \sum_{j=1}^{S} z^{L_j}.$$

Therefore $\phi_f \in \mathfrak{R}$. Suppose now that $\phi_f \in \mathfrak{R}$. By Lemma 2, (c)

$$\sum_{j=0}^{N} c_j \operatorname{sgn}|f_{n+j}| = 0, \qquad n \geqslant n_0.$$

However, there are exactly 2^N different sequences

$$\operatorname{sgn}|f_n|, \operatorname{sgn}|f_{n+1}|, \ldots, \operatorname{sgn}|f_{n+N-1}|.$$

It follows that the sequence $\{\operatorname{sgn}|f_n|\}$, $n = 0, 1, \ldots$, is periodic, $n \geqslant n_0$. Since

$$I_f = I_{\phi_f},$$

this implies at once Theorem (B), and therefore also Theorem (A).

4. Let $f \in \mathfrak{R}$, by Lemma 2, (b) f is a sum of a polynomial and a finite number of partial fractions corresponding to the distinct poles $z = \alpha_k$, $k = 1, 2, \ldots, N$. A pole at α_k will be called pseudo-rational if $\alpha_k/|\alpha_k|$ is a root of unity, otherwise it will be called pseudo-irrational. We have now a unique decomposition

$$f = P + f_1 + f_2 \tag{3}$$

where P is a polynomial, all the poles of f_1 are pseudo-rational, and those of f_2 are all pseudo-irrational. A function $f \in \mathfrak{R}$ is called itself pseudo-rational if in its decomposition (3) $f_2 \equiv 0$.

Let

$$f = \sum_{n=0}^{\infty} f_n z^n \in \mathfrak{R}, \qquad g = \sum_{n=0}^{\infty} g_n z^n \in \mathfrak{R},$$

and let f_n and g_n be real for all n. Put

$$f \cup g = \sum_{n=0}^{\infty} \max(f_n, g_n) z^n, f \cap g = \sum_{n=0}^{\infty} \min(f_n, g_n) z^n. \tag{4}$$

We can state now our principal result.

THEOREM 1. *Let*

$$f = \sum_{n=0}^{\infty} f_n z^n \in \mathfrak{R}$$

and let f_n be real for all n. If f is pseudo-rational then $\chi_f \in \mathfrak{R}$. The set $\mathfrak{P}$ of all pseudo-rational functions with real coefficients is a sub-algebra of $\mathfrak{R}$, over the real numbers, under the ordinary addition and the multiplication of (1), *and it is also a lattice under the operations of* (4).

5. We need first a preliminary

LEMMA 3. *Let*

$$E(n) = \sum_{k=1}^{N} P_k(n)\alpha_k^{-n}$$

be an exponential polynomial, real for $n = 0, 1, \ldots$. Let the α_k be roots of unity. Then $\{\operatorname{sgn} E(n)\}$, $n = 0, 1, \ldots$, is a periodic sequence, $n \geqslant n_0$, and $\min \{|E(n)| \; |E(n) \neq 0\} \geqslant c > 0$.

We have

$$E(n) = \sum_{k=1}^{N} \sum_{j=0}^{M} a_{kj} n^j \alpha_k^{-n} \tag{5}$$

where $M = \max_k \deg P_k$; M is called the degree of E. One can write (5) as

$$E(n) = \sum_{j=0}^{M} F_j(n) n^j \tag{6}$$

where

$$F_j(n) = \sum_{k=1}^{N} a_{kj}\alpha_k^{-n}.$$

By the hypothesis $\alpha_k = \exp 2\pi i \, p_k/q_k$, $0 \leqslant p_k < q_k$, $(p_k, q_k) = 1$. Let $Q = \text{l.c.m.} \{q_k\}$, then $F_j(n) = F_j(n + Q)$ for all n and j. We can also show that $F_j(n)$ is real for all n and j; this follows by observing that with each pair α_k, $P_k = \sum a_{kj} n^j$ in E there is associated the conjugate pair $\bar{\alpha}_k$, $\bar{P}_k = \sum \bar{a}_{kj} n^j$.

The lemma will be proved by induction on the degree M of E. Suppose first that $M = 0$, then

$$E(n) = F_0(n) = \sum_{k=1}^{N} a_{k0}\alpha_k^{-n}$$

so that $\{E(n)\}$, $n = 0, 1, \ldots$, is a periodic sequence of real numbers with period Q. Therefore the lemma holds here. Suppose now that the lemma has been established for exponential polynomials of degree $\leqslant M$, and let deg $E = M + 1$. Then

$$E(n) = F_{M+1}(n)\, n^{M+1} + E_1(n) \tag{7}$$

where $F_{M+1}(n)$ is real for all n and not identically zero, and deg $E_1 \leqslant M$. Let Q be the common period of $F_0, F_1, \ldots, F_{M+1}$ and consider the set

$$S = \{F_{M+1}(0), F_{M+1}(1), \ldots, F_{M+1}(Q)\}.$$

If no member of S vanishes then

$$\min_n |F_{M+1}(n)| = \min_{0 \leqslant n \leqslant Q-1} |F_{M+1}(n)| = c > 0, \tag{8}$$

and the first term on the right in (7) dominates the whole right-hand side since $|E_1(n)| = 0(n^M)$. Now the periodicity of $F_{M+1}(n)$ and the condition (8) imply that the lemma holds in this case.

Suppose now that some members of S vanish. For $n \in I$ let $n \in A$ if $n \equiv n_1 \pmod{Q}$ and $F_{M+1}(n_1) = 0$, $0 \leqslant n_1 < Q$; otherwise let $n \in B$. When n is restricted to B the lemma holds as before; when $n \in A$, $E(n) = E_1(n)$ and the lemma holds by the induction assumption since $\deg E_1 < M$. This concludes the proof.

6. We prove now Theorem 1. Let $f = \sum_0^\infty f_n z^n$ be a pseudo-rational function and let f_n be real for all n. By Lemma 2, (b) we have

$$f(z) = P(z) + \sum_{r=1}^{R} \sum_{k=1}^{N} \sum_{j=1}^{M} A_{rkj}(\alpha_{rk} - z)^{-j} = P(z) + \sum_{r=1}^{R} g_r(z) \tag{9}$$

where $|\alpha_{rk}| = a_r$ and $0 < a_1 < a_2 < \ldots < a_R$. That is, we order the partial fractions according to the increasing absolute value of the poles. R will be called the order of f. Since the presence of P in (9) influences only a finite number of coefficients we assume without loss of generality that $P \equiv 0$.

We show first that $\chi_f \in \mathfrak{R}$. The proof will proceed by induction on the order R of f. Let $R = 1$, then $f = g_1(z)$ and so

$$f_n = a_1^{-n} E_1(n) \tag{10}$$

where $E_1(n)$ satisfies the conditions of Lemma 3. It follows that $\{\operatorname{sgn} E_1(n)\}$, $n = 0, 1, \ldots$, is a periodic sequence, $n \geqslant n_0$, which implies immediately that $\chi_f \in \mathfrak{R}$. Suppose now $\chi_f \in \mathfrak{R}$ for any function f of order $\leqslant R$, satisfying the conditions. Let f be a function of order $R + 1$, then

$$f(z) = g_1(z) + h(z)$$

where the order of h is $\leqslant R$ and the absolute value a_1 of the poles of g_1 is less than that of any pole of h. Let

$$g_1(z) = \sum_{n=0}^{\infty} g_{n1} z^n, \; h(z) = \sum_{n=0}^{\infty} h_n z^n,$$

then $f_n = g_{n1} + h_n$. Suppose that $g_{n1} \neq 0$ for all n. By Lemma 3 it follows easily that $h_n = 0(g_{n1})$ for large n and therefore $\operatorname{sgn} f_n = \operatorname{sgn} g_{n1}$, $r \geqslant n_0$. However, by the induction assumption $\{\operatorname{sgn} g_{n1}\}$, $n = 0, 1, \ldots$, is a periodic sequence, $n \geqslant n_0$. Hence $\{\operatorname{sgn} f_n\}$, $n = 0, 1, \ldots$, is a periodic sequence, $n \geqslant n_0$, and $\chi_f \in \mathfrak{R}$.

Suppose now that $g_{n1} = 0$ for infinitely many n, and let $n \in A$ if $g_{n1} = 0$, $n \in B$ otherwise. Much in the same way as in the proof of Lemma 3 we show

that $\{\operatorname{sgn} f_n\}$ is a periodic sequence when n is restricted to A, and also when n is restricted to B, which again implies that $\chi_f \in \mathfrak{R}$.

Furthermore, it is easy to show that χ_f must have the following form

$$\chi_f(z) = P(z) + e(z) - e(z^L)Q(z)$$

where

$$Q(z) = \sum_{j=0}^{L-1} \epsilon_j z^j$$

and $\epsilon_j = 0, 1$ or -1. It follows that not only $\chi_f \in \mathfrak{R}$ but actually $\chi_f \in \mathfrak{P}$.

We proceed now with the rest of the proof. It is clear that $\mathfrak{P}$ is closed under addition and multiplication by real numbers. We show next that $f \circ g \in \mathfrak{P}$ if $f, g \in \mathfrak{P}$. Although this follows immediately from Lemma 2, (d) the following proof supplies a closed explicit representation for $f \circ g$. As in Lemma 2, (b) let

$$f(z) = P(Z) + \sum_{k=1}^{M} \sum_{j=1}^{N} A_{jk}(\alpha_k - z)^{-j},$$

$$g(z) = P_1(z) + \sum_{k=1}^{M_1} \sum_{j=1}^{N_1} B_{jk}(\beta_k - z)^{-j},$$

then

$$(11) \quad f \circ g = Q(z) + \sum_{k=1}^{M} \sum_{j=1}^{N} \sum_{k_1=1}^{M_1} \sum_{j_1=1}^{N_1} A_{jk}B_{j_1k_1}(\alpha_k - z)^{-j} \circ (\beta_{k_1} - z)^{-j_1}$$

where Q is a polynomial. Now

$$(12) \quad (\alpha_k - z)^{-j} \circ (\beta_{k_1} - z)^{-j_1} = \sum_{n=0}^{\infty} \binom{n+j-1}{n}\binom{n+j_1-1}{n} z^n / \alpha_k^{n+j} \beta_{k_1}^{n+j_1}.$$

Let constants γ_{pqs}, $s = 1, 2, \ldots, p+q-1$, be determined so that

$$\binom{n+p-1}{n}\binom{n+q-1}{n} = \sum_{s=1}^{p+q-1} \gamma_{pqs}\binom{n+s-1}{n}$$

identically in n. Then by (12)

$$(13) \qquad (\alpha_k - z)^{-j} \circ (\beta_{k_1} - z)^{-j_1} = \sum_{s=1}^{j_1+j-1} \gamma_{jj_1s}\alpha_k^{s-j}\beta_{k_1}^{s-j_1}(\alpha_k\beta_{k_1} - z)^{-s}.$$

By putting together (11) and (13) we obtain an explicit representation of $f \circ g$ and see at once that $f \circ g \in \mathfrak{P}$, since

$$\frac{\alpha_k\beta_{k_1}}{|\alpha_k\beta_{k_1}|} = \frac{\alpha_k}{|\alpha_k|} \cdot \frac{\beta_{k_1}}{|\beta_{k_1}|}.$$

By (4)

$$\begin{aligned} f \cup g &= 1/2 \sum_{n=0}^{\infty} [f_n + g_n + (f_n - g_n)\operatorname{sgn}(f_n - g_n)]z^n \\ &= 1/2[f + g + (f - g)\chi_{f-g}], \end{aligned}$$

and $f \cap g = f + g - f \cup g$. Since $f - g \in \mathfrak{P}$ implies $\chi_{f-g} \in \mathfrak{P}$, it follows that if $f, g \in \mathfrak{P}$ then $f \cup g \in \mathfrak{P}$ and $f \cap g \in \mathfrak{P}$. This completes the proof.

The author acknowledges gratefully suggestions and criticism of Professor K. Mahler of Manchester University.

References

1. C. Lech, Ark. Mat., *2* (1953), 417–21.
2. K. Mahler, Cambr. Phil. Soc., *52* (1956), 39–48.
3. E. C. Titchmarsh, *The theory of functions* (Oxford 1939).

McGill University

CERTAIN BILATERAL HYPERGEOMETRIC IDENTITIES OF CAYLEY AND ORR TYPE

NIRMALA AGARWAL

1. Recently I **(1)** gave some new basic hypergeometric identities of the Cayley and Orr type with the help of a certain basic differential operator. The present paper deals with some bilateral generalizations of those identities together with certain new identities of the same type. In § 4 is indicated how the generalizations of Orr's identities given recently by Shukla **(8,** Theorems I, II**)** may be connected with each other. Later in § 5 certain general expansions of hypergeometric functions are deduced. The following notation has been used throughout this paper:

$$(q^a; n) = (a; n) = (1 - q^a)(1 - q^{a+1}) \dots (1 - q^{a+n-1}), \ (a; o) = 1$$

$$(q^a; -n) = (a; -n) = (-)^n q^{\frac{1}{2}n(n+1)}/q^{na}(q^{1-a}; n), \qquad |q| < 1$$

$$(a)_{-n} = (-)^n/(1 - a)_n,$$

$${}_r\Psi_r\left(\begin{matrix} a_1, a_2, \dots, a_r \\ b_1, b_2, \dots, b_r \end{matrix}; x\right) = \sum_{n=-\infty}^{\infty} \frac{(a_1; n)(a_2; n) \dots (a_r; n)\, x^n}{(b_1; n)(b_2; n) \dots (b_r; n)},$$

where, for convergence, $|x| < 1$, $|b_1 b_2 \dots b_r| < |a_1 a_2 \dots a_r x| < 1$.

$${}_rH_r\left(\begin{matrix} a_1, a_2, \dots, a_r \\ b_1, b_2, \dots, b_r \end{matrix}; x\right) = \sum_{n=-\infty}^{\infty} \frac{(a_1)_n (a_2)_n \dots (a_r)_n}{(b_1)_n (b_2)_n \dots (b_r)_n} x^n, \qquad |x| = 1$$

$${}_r\Phi_s\left(\begin{matrix} a_1, a_2, \dots a_r \\ b_1, b_2, \dots, b_s \end{matrix}; x\right) = \sum_{n=0}^{\infty} \frac{(a_1; n)(a_2; n) \dots (a_r; n)}{(1; n)(b_1; n)(b_2; n) \dots (b_s; n)} x^n, \qquad |x| < 1$$

$${}_rF_s\left(\begin{matrix} a_1, a_2, \dots, a_r \\ b_1, b_2, \dots, b_s \end{matrix}; x\right) = \sum_{n=0}^{\infty} \frac{(a_1)_n (a_2)_n \dots (a_r)_n}{n!(b_1)_n (b_2)_n \dots (b_s)_n} x^n, \qquad |x| < 1$$

$$\Gamma\left(\begin{matrix} a_1, a_2, \dots, a_m \\ b_1, b_2, \dots, b_m \end{matrix};\right) = \frac{\Gamma(a_1)\Gamma(a_2) \dots \Gamma(a_m)}{\Gamma(b_1)\Gamma(b_2) \dots \Gamma(b_m)},$$

$$\Gamma_m\left(\begin{matrix} a, b \\ c, d \end{matrix};\right) = \frac{(a)_m (b)_m}{(c)_m (d)_m},$$

$$(\delta; n) = (1 - q^\delta)(1 - q^{\delta+1}) \dots (1 - q^{\delta+n-1}),$$

where $\delta \equiv x\, \partial/\partial x$, and

$$\Delta_q(h) = \frac{\Gamma_q(q^{\delta+h})}{\Gamma_q(q^\delta)} = \frac{\Gamma_q(\delta + h)}{\Gamma_q(h)}$$

Received December 15, 1958.

where $\Gamma_q(x)$ is a basic gamma function defined by Jackson **(7)** and

$$\Delta(h) = \frac{\Gamma(\delta + h)}{\Gamma(h)}.$$

2. Three bilateral hypergeometric identities. We now proceed to prove the following three identities that:

$$(2.1)\quad (c;m)(d-b;m)(a+c-2m;m)\,\Delta_q(c+m) \times {}_1\Psi_1\left(\begin{matrix} d-b+m; \\ 1+m \end{matrix} x\right) {}_2\Psi_2\left(\begin{matrix} a+c-m, b; \\ 1+m, c \end{matrix} xq^{-a-b+2m}\right)$$

= the same expression with c and d interchanged.

$$(2.2)\quad (f-b;m)(d;m)(1-a;m)(e-c;m)\,\Delta_q(d+m) \times {}_1\Psi_1\left(\begin{matrix} f-b+m; \\ 1+m \end{matrix} x\right) {}_3\Psi_3\left(\begin{matrix} a, b, e-c+m; \\ 1+m, d, e \end{matrix} xq^{f-b}\right)$$

$$= (d-b;m)(f;m)(1-c;m)(e-a;m)\,\Delta_q(f+m) \times {}_1\Psi_1\left(\begin{matrix} d-b+m; \\ 1+m \end{matrix} x\right) {}_3\Psi_3\left(\begin{matrix} c, b, e-a+m; \\ 1+m, e, f \end{matrix} xq^{d-b}\right)$$

provided $a + f = c + d$.

$$(2.3)\quad \frac{(c;m)(c';m)}{(c-a;m)(c'-b';m)}\,\Delta_q(c+m)\Delta_q(c'+m) \times {}_2\Psi_2\left(\begin{matrix} a, b; \\ 1+m, c \end{matrix} xq^{c-a-b+m}\right) {}_2\Psi_2\left(\begin{matrix} a', b'; \\ 1+m, c' \end{matrix} x\right)$$

$$= \frac{(1-a-a';m)(1-b-b';m)}{(1-a';m)(1-b;m)}\,q^{(a+b')m}\,\Delta_q(a+a')\,\Delta_q(b+b') \times {}_2\Psi_2\left(\begin{matrix} b', c-a+m; \\ 1+m, b+b'-m \end{matrix} x\right) {}_2\Psi_2\left(\begin{matrix} c'-b'+m, a; \\ 1+m, a+a'-m \end{matrix} x\,q^{a'+b'-c'-m}\right)$$

provided $a + a' + b + b' = c + c' + 2m$.

The identities (2.1, 2.2, and 2.3) are generalizations of certain earlier results **(1**, 2.1, 2.2, 2.3**)**.

Proof of 2.1. Consider the known identity **(1**, 2.1**)**, namely, that

$$(2.4)\qquad \Delta_q(c)\,{}_1\Phi_0(d-b;x)\;{}_2\Phi_1\left(\begin{matrix} a+c, b; \\ c \end{matrix} xq^{-a-b}\right)$$

equals the same expression with c and d interchanged.

Comparing the coefficients of x^n on both the sides we get the transformation

$$(2.5)\quad (c;n)(d-b;n)\ {}_3\Phi_2\left(\begin{matrix}a+c,\ b,\ -n;\\ c,\ 1+b-d-n\end{matrix}\ q^{1-a-d}\right)$$
$$= (d;n)(c-b;n)\ {}_3\Phi_2\left(\begin{matrix}a+d,\ b,\ -n;\\ d,\ 1+b-c-n\end{matrix}\ q^{1-a-c}\right).$$

Replacing n, a, b, c, and d respectively by $2m+n$, $a-m$, $b-m$, $c-m$, $d-m$ in (2.5) we find that

$$(2.6)\quad (c;m+n)(d-b;m+n)(a+c-2m;m)$$
$$\times\ {}_3\Psi_3\left(\begin{matrix}a+c-m,\ b,\ -m-n;\\ 1+m,\ c,\ 1+b-d-m-n\end{matrix}\ q^{1-a-d+2m}\right)$$

equals the same expression with c and d interchanged.* Hence on comparing the coefficients of x^n and using the relation (2.6) we find that

$$(c;m)(d-b;m)(a+c-2m;m)\ \Delta_q(c+m)$$
$$\times\ {}_1\Psi_1\left(\begin{matrix}d-b+m;\\ 1+m\end{matrix}\ x\right)\ {}_2\Psi_2\left(\begin{matrix}a+c-m,\ b;\\ 1+m,\ c\end{matrix}\ x\,q^{-a-b+2m}\right)$$

equals the same expression with c and d interchanged, which proves (2.1). Putting $m=0$ (2.1) gives (2.4).

Proceeding exactly in the above manner we can prove the identities (2.2) and (2.3). Putting $m=0$ in (2.2) and (2.3) we get back to the known identities due to Agarwal **(1**, 2.2, and 2.3**)**.

3. Certain new identities and their generalizations. In this section we prove three new identities and later deduce their bilateral generalizations. The identities are

$$(3.1)\quad \Delta(1+a-c)\ {}_1F_0(e-c;x)\ {}_3F_2\left(\begin{matrix}a,\ b,\ c;\\ 1+a-b,\ 1+a-c\end{matrix}\ x\right)$$
$$= \Delta(e)\ {}_1F_0(1+a-2c;x)\ {}_4F_3\left(\begin{matrix}a-2b,\ 1+\tfrac{1}{2}a-b,\ -b,\ c;\\ \tfrac{1}{2}a-b,\ 1+a-b,\ e\end{matrix}\ x\right)$$

and

$$(3.2)\quad \Delta(1+a-c)\ {}_1F_0(e-c;x)\ {}_4F_3\left(\begin{matrix}a,\ \tfrac{1}{2}a+1,\ b,\ c;\\ \tfrac{1}{2}a,\ 1+a-b,\ 1+a-c\end{matrix}\ x\right)$$
$$= \Delta(e)\ {}_1F_0(1+a-2c;x)\ {}_3F_2\left(\begin{matrix}a-2b,\ -b,\ c;\\ 1+a-b,\ e\end{matrix}\ x\right),$$

*The limiting case as $q\to 1$ of (2.6) can be obtained directly by putting $c=m+n+1$ and replacing $2-e$, $2-f$, b, d, and a respectively by c, d, $1-b$, $1-m$, and $1+a-2m$ in a known result due to M. Jackson **(6**, p. 34**)**.

provided $1 + a - c - e = 2b$ in (3.1) and (3.2), and

$$(3.3)\quad \Delta(1+a-c)\,{}_1F_0(e-c;x)\,{}_4F_3\left(\begin{matrix}a, \frac{1}{2}a+1, b, c; x\\ \frac{1}{2}a, 1+a-b, 1+a-c\end{matrix}\right)$$
$$= \Delta(e)\,{}_1F_0(1+a-2c;x)\,{}_4F_3\left(\begin{matrix}a-2b-1, \frac{1}{2}a+\frac{1}{2}-b, -b-1, c; x\\ \frac{1}{2}a-\frac{1}{2}-b, 1+a-b, e\end{matrix}\right)$$

provided $a - c - e = 2b$.

Proof of (3.1). It is easy to see that for suitably restricted parameters we have **(4)**

$$\frac{\Gamma(\delta+c)\Gamma(d-c)}{\Gamma(\delta+d)} f(x) = \int_0^1 u^{c-1}(1-u)^{d-c-1} f(xu)\,du.$$

Let us replace c and d respectively by $1 + a - c$ and e and take

$$f(x) = {}_1F_0(e-c;x)\,{}_3F_2\left(\begin{matrix}a, b, c; x\\ 1+a-b, 1+a-c\end{matrix}\right).$$

Then the right-hand side becomes

$$\int_0^1 u^{a-c}(1-u)^{e+c-a-2}(1-ux)^{c-e}\,{}_3F_2\left(\begin{matrix}a, b, c; xu\\ 1+a-b, 1+a-c\end{matrix}\right) du.$$

Expanding the ${}_3F_2$ series and interchanging the order of integration and summation (which is easily justifiable), we have

$$\sum_{r=0}^{\infty} \frac{(a)_r(b)_r(c)_r}{r!(1+a-b)_r(1+a-c)_r} x^r \int_0^1 u^{a+r-c}(1-u)^{e+c-a-2}(1-ux)^{c-e}\,du$$
$$= \sum_{r=0}^{\infty} \frac{(a)_r(b)_r(c)_r x^r}{r!(1+a-b)_r(1+a-c)_r} \cdot \frac{\Gamma(1+a-c+r)\Gamma(e+c-a-1)}{\Gamma(e+r)}$$
$${}_2F_1\left(\begin{matrix}e-c, 1+a-c+r; x\\ e+r\end{matrix}\right).$$

Using Euler's identity (Tract 1, 1.2, 2.) we get

$$(3.4)\quad \frac{\Gamma(1+a-c)\Gamma(e+c-a-1)}{\Gamma(e)}\,{}_1F_0(1+a-2c;x)$$
$$\sum_{r=0}^{\infty} \frac{(a)_r(b)_r(c)_r}{r!(1+a-b)_r(e)_r} x^r\,{}_2F_1\left(\begin{matrix}c+r, e+c-a-1; x\\ e+r\end{matrix}\right).$$

Now, we have the transformation

$${}_4F_3\left(\begin{matrix}a-2b, \frac{1}{2}a+1-b, -b, c; x\\ \frac{1}{2}a-b, 1+a-b, e\end{matrix}\right)$$
$$= \sum_{r=0}^{\infty} \frac{(a)_r(b)_r(c)_r}{r!(1+a-b)_r(e)_r} x^r\,{}_2F_1\left(\begin{matrix}c+r, e+c-a-1; x\\ e+r\end{matrix}\right)$$

provided $1 + a - c - e = 2b$, which can easily be obtained by collecting the coefficients of x^n and using the known summation theorem **(2, §§ 4.5, 1.2)**. Hence using this transformation in (3.4) we have the required identity (3.1).

To prove (3.2) and (3.3) we proceed exactly as above with

$$f(x) = {}_1F_0(e - c; x)\ {}_4F_3\left(\begin{matrix} a, \frac{1}{2}a + 1, b, c; \\ \frac{1}{2}a, 1 + a - b, 1 + a - c \end{matrix} x\right),$$

and use the transformations **(2, §§ 4.5, 1.3, 1.4)** giving the sum of a nearly-poised ${}_4F_3$.

We can also obtain the basic analogue of the identity (3.3) in the form

$$(3.5)\quad \Delta_q(1 + a - c)\ {}_1\Phi_0(q^{e-c}; x)\ {}_5\Phi_4\left(\begin{matrix} q^a, q^{\frac{1}{2}a+1}, -q^{\frac{1}{2}a+1}, q^b, q^c; \\ q^{\frac{1}{2}a}, -q^{\frac{1}{2}a}, q^{1+a-b}, q^{1+a-c} \end{matrix} xq^{a-2b-2c}\right)$$

$$= \Delta_q(e)\,{}_1\Phi_0(q^{1+a-2c}; x)\ {}_5\Phi_4\left(\begin{matrix} q^{a-2b-1}, q^{\frac{1}{2}a+\frac{1}{2}-b}, -q^{\frac{1}{2}a+\frac{1}{2}-b}, q^{-b-1}, q^c; \\ q^{\frac{1}{2}a-\frac{1}{2}-b}, -q^{\frac{1}{2}a-\frac{1}{2}-b}, q^{1+a-b}, q^e \end{matrix} xq^{1+a-2c}\right)$$

provided $a - c - e = 2b$.

To prove (3.5) we use the basic integral

$$(3.6)\quad \frac{\Gamma_q(\delta + c)\Gamma_q(d - c)}{\Gamma_q(\delta + d)}\,\Phi(x) = \int_0^1 u^{c-1}(1 - uq)^{d-c-1}\Phi(xu)\,d(qu)$$

used in an earlier paper as well **(1)**, where $(1 - q^a x)^{-a}$ means the basic binomial expansion

$$1 + \frac{(1 - q^a)}{(1 - q)}x + \frac{(1 - q^a)(1 - q^{a+1})}{(1 - q)(1 - q^2)}x^2 + \ldots,$$

or ${}_1\Phi_0\,(a; x)$.

Replace c and d respectively by $1 + a - c$ and e in (3.6) and take

$$\Phi(x) = {}_1\Phi_0(q^{e-c}; x)\ {}_5\Phi_4\left(\begin{matrix} q^a, q^{\frac{1}{2}a+1}, -q^{\frac{1}{2}a+1}, q^b, q^c; \\ q^{\frac{1}{2}a}, -q^{\frac{1}{2}a}, q^{1+a-b}, q^{1+a-c} \end{matrix} xq^{a-2b-2c}\right).$$

Proceeding as for (3.1) we obtain, on using a known summation theorem due to Bailey **(3, § 3 (3))**, the required identity (3.5).

It may be noted that as a consequence of these identities we get certain interesting relations between two terminating nearly-poised series. From (3.1), (3.2), and (3.3) respectively we get

$$(3.7)\quad {}_4F_3\left(\begin{matrix} a, b, c, -n; \\ 1 + a - b, 1 + a - c, 1 + c - e - n \end{matrix}\right)$$

$$= \frac{(1 + a - 2c)_n(e)_n}{(1 + a - c)_n(e - c)_n}\ {}_5F_4\left(\begin{matrix} a - 2b, 1 + \frac{1}{2}a - b, -b, c, -n; \\ \frac{1}{2}a - b, 1 + a - b, e, 2c - a - n \end{matrix}\right)$$

provided $1 + a - c - e = 2b$,

$$(3.8)\quad {}_5F_4\left(\begin{matrix} a, \frac{1}{2}a + 1, b, c, -n; \\ \frac{1}{2}a, 1 + a - b, 1 + a - c, 1 + c - e - n \end{matrix}\right)$$

$$= \frac{(1 + a - 2c)_n(e)_n}{(1 + a - c)_n(e - c)_n}\ {}_4F_3\left(\begin{matrix} a - 2b, -b, c, -n; \\ 1 + a - b, e, 2c - a - n \end{matrix}\right)$$

provided $1 + a - c - e = 2b$, and

$$(3.9)\quad {}_5F_4\left(\begin{matrix} a, \frac{1}{2}a + 1, b, c, -n; \\ \frac{1}{2}a, 1 + a - b, 1 + a - c, 1 + c - e - n \end{matrix}\right) = \frac{(1 + a - 2c)_n (e)_n}{(1 + a - c)_n (e - c)_n} {}_5F_4\left(\begin{matrix} a - 2b - 1, \frac{1}{2}a + \frac{1}{2} - b, -b - 1, c, -n; \\ \frac{1}{2}a - \frac{1}{2} - b, 1 + a - b, e, 2c - a - n \end{matrix}\right)$$

provided $a - c - e = 2b$.

The basic analogue of (3.9) may be written as (from 3.5)

$$(3.10)\quad {}_6\Phi_5\left(\begin{matrix} q^a, q^{\frac{1}{2}a+1}, -q^{\frac{1}{2}a+1}, q^b, q^c, q^{-n}; q \\ q^{\frac{1}{2}a}, -q^{\frac{1}{2}a}, q^{1+a-b}, q^{1+a-c}, q^{1+c-e-n} \end{matrix}\right) = \frac{(q^{1+a-2c}; n)(q^c; n)}{(q^{1+a-c}; n)(q^{c-e}; n)} {}_6\Phi_5\left(\begin{matrix} q^{a-2b-1}, q^{\frac{1}{2}a+\frac{1}{2}-b}, -q^{\frac{1}{2}a+\frac{1}{2}-b}, q^{-b-1}, q^c, q^{-n}; q \\ q^{\frac{1}{2}a-\frac{1}{2}-b}, -q^{\frac{1}{2}a-\frac{1}{2}-b}, q^{1+a-b}, q^c, q^{2c-a-n} \end{matrix}\right)$$

provided $a - c - e = 2b$.

Next we deduce the bilateral generalizations of the identities (3.1), (3.2), and (3.3). In the known transformation due to Shukla **(8, 2.2)** let us take $M = 3$, $N = 1$, $a_1 = b_1 = 1$ and $c_4 = 0$. This gives us a relation between three non-terminating nearly-poised ${}_4H_4$ series and a terminating ${}_4F_3$ series viz.;

$$(3.11)\quad (1 - E)(1 - F)\,\Gamma\left(\begin{matrix} 1 + E - D, 1 + F - D, D - E, D - F; \\ 2 + a - b - D, 2 + a - c - D, 2 + c - e - D, D - a, D - b, D - c \end{matrix}\right) \times \frac{(D + e - c - 1)_n}{(D)_n} {}_4H_4\left(\begin{matrix} 1 + a - D, 1 + b - D, 1 + c - D, 1 - D - n; \\ 2 - D, 2 + a - b - D, 2 + a - c - D, 2 + c - e - D - n \end{matrix}\right) + \text{idem } (D; E, F)$$
$$= \Gamma\left(\begin{matrix} D, E, F, 2 - D, 2 - E, 2 - F; \\ 1 + a - b, 1 + a - c, 1 + c - e, 1 - a, 1 - b, 1 - c \end{matrix}\right) \times \frac{(e - c)_n}{(1)_n} {}_4F_3\left(\begin{matrix} a, b, c, -n; \\ 1 + a - b, 1 + a - c, 1 + c - e - n \end{matrix}\right).$$

Transform the ${}_4F_3$ series on the right by (3.7) and then replace n, a, b, c, and e respectively by $2m + n$, $a - 2m$, $b - m$, $c - m$, and $e - m$. After some simplification we find that (3.11) may be written as

$$(3.12)\quad (1 - E)(1 - F)\,\Gamma\left(\begin{matrix} 1 + E - D, 1 + F - D, D - E, D - F; \\ 2 + a - b - D - m, 2 + a - c - D - m, 2 + c - e - D, \\ D - a + 2m, D - b + m, D - c + m \end{matrix}\right) \times \frac{(D + e - c - 1)_{2m}}{(D)_{2m}} {}_1H_1\left(\begin{matrix} D + e - c - 1 + 2m; x \\ D + 2m \end{matrix}\right) \times$$

$$
{}_3H_3\left(\begin{matrix}1+a-D-2m, 1+b-D-m, 1+c-D-m;\\ 2-D, 2+a-b-D-m, 2+a-c-D-m\end{matrix}\;x\right)
$$

$$
+ \text{idem } (D; E, F)
$$

$$
= \Gamma\left(\begin{matrix}D, E, F, 2-D, 2-E, 2-F;\\ 1+a-b-m, 1+a-c-m, 1+c-e, 1-a+2m,\\ 1-b+m, 1-c+m\end{matrix}\right)
$$

$$
\times \Gamma_m\left(\begin{matrix}e, a-2b, \tfrac{1}{2}a+1-b, 1-c, -b+m, 1+a-2c;\\ 1, \tfrac{1}{2}a-b, b-a, c-a, 1+a-c\end{matrix}\right)
$$

$$
\times \frac{\Delta(e+m)}{\Delta(1+a-c+m)}
$$

$$
\times {}_4H_4\left(\begin{matrix}a-2b+m, \tfrac{1}{2}a+1-b+m, -b+2m, c;\\ 1+m, \tfrac{1}{2}a-b+m, 1+a-b, e\end{matrix}\;x\right)
$$

$$
{}_1H_1\left(\begin{matrix}1+a-2c+m\\ 1+m\end{matrix};\,x\right),
$$

provided $1 + a - c - e = 2b - 2m$. (3.12) reduces to (3.1) when $D = 1$ and $m = 0$.

In exactly the same manner bilateral generalizations of the identities (3.2) and (3.3) may be written in the form

(3.13) $(1-E)(1-F)(1-G)$

$$
\Gamma\left[\begin{matrix}1+E-D, 1+F-D, 1+G-D, D-E, D-F,\\ 1+\tfrac{1}{2}a-D-m, 2+a-b-D-m, 2+a-c-D-m, 2+c-e-D,\\ D-G;\\ D-a+2m, D-\tfrac{1}{2}a-1+m, D-b+m, D-c+m\end{matrix}\right]
$$

$$
\times \frac{(D+e-c-1)_{2m}}{(D)_{2m}}\,{}_1H_1\left(\begin{matrix}D+e-c-1+2m;\\ D+2m\end{matrix}\;x\right)
$$

$$
{}_4H_4\left(\begin{matrix}1+a-D-2m, 2+\tfrac{1}{2}a-D-m, 1+b-D-m, 1+c-D-m;\\ 2-D, 1+\tfrac{1}{2}a-D-m, 2+a-b-D-m, 2+a-c-D-m\end{matrix}\;x\right)
$$

$$
+ \text{idem } (D; E, F, G)
$$

$$
= \Gamma\left(\begin{matrix}D, E, F, G, 2-D, 2-E, 2-F, 2-G;\\ 1+a-b-m, 1+a-c-m, 1+c-e, \tfrac{1}{2}a-m, 1-a+2m,\\ -\tfrac{1}{2}a+m, 1-b+m, 1-c+m\end{matrix}\right)
$$

$$
\times \Gamma_m\left(\begin{matrix}e, a-2b, -b+m, 1-c, 1+a-2c\\ 1, b-a, c-a, 1+a-c\end{matrix}\right)\frac{\Delta(e+m)}{\Delta(1+a-c+m)}
$$

$$
\times {}_1H_1\left(\begin{matrix}1+a-2c+m;\\ 1+m\end{matrix}\;x\right)\,{}_3H_2\left(\begin{matrix}a-2b+m, -b+2m, c;\\ 1+m, 1+a-b, e\end{matrix}\;x\right)
$$

provided $1 + a - c - e = 2b - 2m$,

(3.14)

$$= \Gamma\left(\begin{matrix} D, E, F, G, 2 - D, 2 - E, 2 - F, 2 - G; \\ 1 + a - b - m, 1 + a - c - m, 1 + c - e, \tfrac{1}{2}a - m, 1 - a + 2m, \\ -\tfrac{1}{2}a + m, 1 - b + m, 1 - c + m \end{matrix}\right)$$

$$\times \Gamma_m\left(\begin{matrix} e, 1 + a - 2c, a - 2b - 1, -b - 1 + m, 1 - c, \tfrac{1}{2}a + \tfrac{1}{2} - b \\ 1, b - a, c - a, 1 + a - c, \tfrac{1}{2}a - \tfrac{1}{2} - b \end{matrix}\right)$$

$$\frac{\Delta(e + m)}{\Delta(1 + a - c + m)}$$

$$\times {}_1H_1\left(\begin{matrix} 1 + a - 2c + m \\ 1 + m \end{matrix}; x\right)$$

$$\times {}_4H_4\left(\begin{matrix} a - 2b + m - 1, \tfrac{1}{2}a + \tfrac{1}{2} - b + m, -b - 1 + 2m, c \\ 1 + m, \tfrac{1}{2}a - \tfrac{1}{2} - b + m, 1 + a - b, e \end{matrix}; x\right)$$

provided $a - c - e = 2b - 2m$. Putting $D = 1$ and $m = 0$ in (3.13) and (3.14) we get back to the identities (3.1) and (3.2).

4. Next we show how the bilateral generalizations due to Shukla **(8**, Theorems I, II**)** of Orr's identities (Tract, § 10.1 (2 and 3)) may be deduced from each other by the use of the following identity:

(4.1)

$$(1 - a)_m(1 - b)_m(1 - a')_m(1 - b')_m {}_2H_2\left(\begin{matrix} a, b \\ 1 + m, c \end{matrix}; x\right) {}_2H_2\left(\begin{matrix} a', b' \\ 1 + m, c' \end{matrix}; x\right)$$

$$= (c - a)_m(c - b)_m(c' - a')_m(c' - b')_m$$

$${}_2H_2\left(\begin{matrix} c - a + m, c - b + m \\ 1 + m, c \end{matrix}; x\right) {}_2H_2\left(\begin{matrix} c' - a' + m, c' - b' + m \\ 1 + m, c' \end{matrix}; x\right)$$

with $a + a' + b + b' = c + c' + 2m$.

The identity (4.1) may be obtained from the known identity due to Chaundy **(4**, 25**)**.

The identities due to Shukla can also be written in the form

(4.2)
$$(1 - E)\,\Gamma\left(\begin{matrix} 1 + E - D, D - E; \\ 1 + 2c - D - 2m, 3/2 + a + b - c - D - m, \\ D - 2b + 2m, D - 2a + 2m \end{matrix}\right)$$

$$\times \frac{(c + D - a - b + \tfrac{1}{2} + m)_{2m}}{(D)_{2m}} {}_1H_1\left(\begin{matrix} c + D - a - b - \tfrac{1}{2} + 3m \\ D + 2m \end{matrix}; x\right)$$

$${}_2H_2\left(\begin{matrix} 1 + 2a - D - 2m, 1 + 2b - D - 2m \\ 2 - D, 1 + 2c - D - 2m \end{matrix}; x\right) + \text{idem } (D; E)$$

$$= \Gamma\begin{bmatrix} D, E, 2-D, 2-E; \\ 2c-2m, \frac{1}{2}+a+b-c-m, 1-2a+2m, 1-2b+2m \end{bmatrix}$$

$$\Gamma_m\begin{bmatrix} \frac{1}{2}+c-a, \frac{1}{2}+c-b, 1+c, 1-a, 1-b; \\ 1, 1, \frac{1}{2}+c, \frac{1}{2}+c, 1-c, \frac{1}{2}-c \end{bmatrix}$$

$$\frac{\Delta(c+1+m)}{\Delta(c+\frac{1}{2}+m)}\, {}_2H_2\left(\begin{matrix} a, b \\ 1+m, c \end{matrix}; x\right) {}_2H_2\left(\begin{matrix} c-a+\frac{1}{2}+m, c-b+\frac{1}{2}+m \\ 1+m, c+1 \end{matrix}; x\right)$$

and

$$(4.3)\quad (1-E)\,\Gamma\left(\begin{matrix} 1+E-D, D-E; \\ 2c-D-2m, 3/2+a+b-c-D-m, \\ 1+D-2a+2m, D-2b+2m \end{matrix}\right)$$

$$\times \frac{(c+D-a-b-\frac{1}{2}+m)_{2m}}{(D)_{2m}}\, {}_1H_1\left(\begin{matrix} c+D-a-b-\frac{1}{2}+3m \\ D+2m \end{matrix}; x\right)$$

$${}_2H_2\left(\begin{matrix} 2a-2m-D, 2b+1-D-2m \\ 2-D, 2c-2m-D \end{matrix}; x\right) + \text{idem } (D; E)$$

$$= \Gamma\left(\begin{matrix} D, E, 2-D, 2-E; \\ 2c-2m-1, \frac{1}{2}+a+b-c-m, 2-2a+2m, 1-2b+2m \end{matrix}\right)$$

$$\Gamma_m\left(\begin{matrix} \frac{1}{2}+c-a, c-\frac{1}{2}-b, 1-a, 1-b; \\ 1, 1, 3/2-c, c-\frac{1}{2}, 1-c \end{matrix}\right) \frac{\Delta(c+m)}{\Delta(c-\frac{1}{2}+m)}\, {}_2H_2\left(\begin{matrix} a, b \\ 1+m, c \end{matrix}; x\right)$$

$${}_2H_2\left(\begin{matrix} c-a+\frac{1}{2}+m, +c-b-\frac{1}{2}+m \\ 1+m, c \end{matrix}; x\right).$$

Now let $q \to 1$ in (2.3) and then use the identity (4.1); to transform the right-hand side put $a + a' = b + b' = c + \frac{1}{2} + m$, and $c' = c + 1$. This gives us the transformation

$$\Gamma_m(c, c+1, \tfrac{1}{2}+c-b, 1-a)\, \frac{\Delta(c+m+1)}{\Delta(c+m+\frac{1}{2})}$$

$$\times {}_2H_2\left(\begin{matrix} a, b \\ 1+m, c \end{matrix}; x\right) {}_2H_2\left(\begin{matrix} c-a+\frac{1}{2}+m, c-b+\frac{1}{2}+m \\ 1+m, c+1 \end{matrix}; x\right)$$

$$= \Gamma_m(\tfrac{1}{2}+c-a, \tfrac{1}{2}+c, \tfrac{1}{2}+c, \tfrac{1}{2}-a, c-b)\, \frac{\Delta(c+\frac{1}{2}+m)}{\Delta(c+m)}$$

$$\times {}_2H_2\left(\begin{matrix} b, a+\frac{1}{2} \\ 1+m, c+\frac{1}{2} \end{matrix}; x\right) {}_2H_2\left(\begin{matrix} c-a+\frac{1}{2}+m, c-b+m \\ 1+m, c+\frac{1}{2} \end{matrix}; x\right).$$

Using (4.2) on the left of the above equation we find that it reduces to (4.3) with $a + \frac{1}{2}$, $c + \frac{1}{2}$ for a and c. Thus (4.3) is connected with (4.2).

5. Certain general hypergeometric expansions. In this section we obtain certain general expansions both for ordinary and bilateral hyper-

geometric series with the help of transformations deduced in previous sections. Before proceeding to the actual deduction of the general expansions we prove a lemma which is a bilateral generalization of a known transformation due to Chaundy **(4, 42)**.

LEMMA. *If*

$$\Psi\left(\begin{matrix}a, \dots \\ 1+m, c, \dots\end{matrix}; xq^{\lambda}\right) \quad \text{and} \quad \Psi\left(\begin{matrix}a', \dots \\ 1+m, c', \dots\end{matrix}; x\right)$$

are two basic bilateral hypergeometric functions (of any order) and h, k, any two suitable constants then

(5.1)

$$\frac{(h+m;m)(k;m)\,\Delta_q(h+2m)}{(k+m;m)(h;m)\,\Delta_q(k+2m)}\Psi\left[\begin{matrix}a, \dots \\ 1+m, c, \dots\end{matrix}; xq^{\lambda}\right]\Psi\left[\begin{matrix}a', \dots \\ 1+m, c', \dots\end{matrix}; x\right]$$

$$= \sum_{r=0}^{\infty} \frac{(k-1;r)(k;2r)(k-h;r)[(h+m;r)]^2(a;r)\dots(a';r)\dots}{(1;r)(h;r)(k-1;2r)[(k+m;2r)]^2(c;r)\dots(c';r)\dots}$$

$$\times x^{2r} q^{r(r-1)+(\lambda+h)r}\,\Psi\left(\begin{matrix}h+m+r, a+r, \dots \\ k+m+2r, 1+m, c+r, \dots\end{matrix}; xq^{\lambda}\right)$$

$$\Psi\left(\begin{matrix}h+m+r, a'+r, \dots \\ k+m+2r, 1+m, c'+r, \dots\end{matrix}; x\right).$$

Proof: It is easily seen that

$$\frac{\Delta_q(h)}{\Delta_q(k)}\Psi\left(\begin{matrix}a, \dots \\ c, \dots\end{matrix}; x\right) = \Psi\left(\begin{matrix}h, a, \dots \\ k, c \dots\end{matrix}; x\right)$$

and

$$q^{(\delta+m)r}\frac{(-\delta-m;r)\Delta_q(h+m)}{(\delta+m+k;r)\Delta_q(k+m)}\Psi\left(\begin{matrix}a, \dots \\ 1+m, c \dots\end{matrix}; xq^{\lambda}\right)$$

$$= \frac{(a;r)\dots(h+m;r)}{(c;r)\dots(k+m;2r)}(-x)^r q^{\frac{1}{2}r(r-1)+\lambda r}$$

$$\Psi\left(\begin{matrix}h+m+r, a+r, \dots \\ k+m+2r, 1+m, c+r, \dots\end{matrix}; xq^{\lambda}\right).$$

Using the above transformation on the right-hand side of (5.1), it becomes

(5.2)
$$\frac{\Gamma_q(\theta+h+m)\Gamma_q(\phi+h+m)}{\Gamma_q(\theta+k+m)\Gamma_q(\phi+k+m)}\left[\frac{\Gamma_q(k+m)}{\Gamma_q(h+m)}\right]^2$$

$$\times \sum_{r=0}^{\infty} \frac{(k-1;r)(k;2r)(k-h;r)(-\theta-m;r)(-\phi-m;r)}{(1;r)(k-1;2r)(h;r)(\theta+k+m;r)(\phi+k+m;r)}\,q^{(\theta+\phi+2m+h)r}$$

$$\times \Psi\left(\begin{matrix}a, \dots \\ 1+m, c, \dots\end{matrix}; xq^{\lambda}\right)\Psi\left(\begin{matrix}a', \dots \\ 1+m, c', \dots\end{matrix}; x\right),$$

where $\theta \equiv x\ \partial/\partial x$ and $\phi \equiv x\ \partial/\partial x$ operate on the first and second series alone respectively and hence $q^{\theta+\phi} = q^{\delta}$. Summing up the above well-poised ${}_6\Phi_5$ series we get the required result (5.1). If we take the limit $q \to 1$ we get the corresponding transformation for ordinary bilateral hypergeometric series, viz.:

$$(5.3)\quad \frac{(h+m)_m(k)_m}{(k+m)_m(h)_m}\frac{\Delta(h+2m)}{\Delta(k+2m)}H\left[\begin{matrix}a,\dots\\1+m,c,\dots\end{matrix};x\right]H\left[\begin{matrix}a',\dots\\1+m,c',\dots\end{matrix};x\right]$$

$$=\sum_{r=0}^{\infty}\frac{(k-1)_r(k)_{2r}(k-h)_r((h+m)_r)^2(a)_r\dots(a')_r\dots}{r!(k-1)_{2r}((k+m)_{2r})^2(h)_r(c)_r\dots(c')_r\dots}x^{2r}$$

$$\times H\left(\begin{matrix}h+m+r,a+r,\dots\\1+m,k+m+2r,c+r,\dots\end{matrix};x\right)H\left(\begin{matrix}h+m+r,a'+r,\dots\\1+m,k+m+2r,c'+r,\dots\end{matrix};x\right).$$

Applications. Applying the transformation (5.1) to the identity (2.1) we get

$$(5.4)\quad {}_1\Psi_1\left(\begin{matrix}d-b+m\\1+m\end{matrix};x\right){}_2\Psi_2\left(\begin{matrix}a+c-m,b\\1+m,c\end{matrix};xq^{-a-b+2m}\right)$$

$$=\frac{(c-b;m)(a+d-2m;m)(d-m;m)}{(d-b;m)(a+c-2m;m)(c-m;m)}$$

$$\times\sum_{r=0}^{\infty}\frac{(c-m-1;r)(c-m;2r)(c-d;r)(d;r)(c-b+m;r)(d+a-m;r)}{(1;r)(c-m-1;2r)(c;2r)(c;2r)(d-m;r)}$$

$$\times(b;r)x^{2r}q^{r(r-1)+(d-a-b+m)r}{}_2\Psi_2\left(\begin{matrix}d+r,c-b+m+r\\1+m,c+2r\end{matrix};x\right)$$

$$\times{}_3\Psi_3\left(\begin{matrix}d+r,a+d-m+r,b+r\\1+m,d+r,c+2r\end{matrix};xq^{-a-b+2m}\right).$$

Similarly, applying the transformation (5.1) to (2.2) and (5.3) to (4.2) and (4.3) one can obtain three other expansions of similar type.

Next, applying the transformation (5.3) for $m = 0$ **(4**, 42**)** to the right-hand side of the identities (3.1), (3.2), and (3.3) respectively, we get the following three expansions

$$(5.5)\quad {}_3F_2\left(\begin{matrix}a,b,c\\1+a-b,1+a-c\end{matrix};x\right)$$

$$=\sum_{r=0}^{\infty}\frac{(2b)_r(1+a-2c)_r(a-2b)_r(\frac{1}{2}a-b+1)_r(-b)_r(c)_r}{r!(a-c+r)_r(1+a-c)_{2r}(\frac{1}{2}a-b)_r(1+a-b)_r}x^{2r}$$

$$\times{}_2F_1\left(\begin{matrix}c+r,2b+r\\1+a-c+2r\end{matrix};x\right)$$

$${}_4F_3\left(\begin{matrix}a-2b+r,\frac{1}{2}a-b+1+r,-b+r,c+r\\\frac{1}{2}a-b+r,1+a-b+r,1+a-c+2r\end{matrix};x\right)$$

with the condition $1 + a - c - e = 2b$,

$$(5.6)\quad {}_4F_3\left(\begin{matrix} a, \frac{1}{2}a + 1, b, c \\ \frac{1}{2}a, 1 + a - b, 1 + a - c \end{matrix}; x\right)$$

$$= \sum_{r=0}^{\infty} \frac{(2b)_r(1 + a - 2c)_r(a - 2b)_r(-b)_r(c)_r}{r!(a - c + r)_r(1 + a - c)_{2r}(1 + a - b)_r} x^{2r}$$

$$\times {}_2F_1\left(\begin{matrix} c + r, 2b + r \\ 1 + a - c + 2r \end{matrix}; x\right) {}_3F_2\left(\begin{matrix} a - 2b + r, -b + r, c + r \\ 1 + a - b + r, 1 + a - c + 2r \end{matrix}; x\right)$$

with $1 + a - c - e = 2b$,

(5.7)

$$= \sum_{r=0}^{\infty} \frac{(2b - 1)_r(1 + a - 2c)_r(a - 2b - 1)_r(\frac{1}{2}a + \frac{1}{2} - b)_r(-b - 1)_r(c)_r}{r!(a - c + r)_r(1 + a - c)_{2r}(\frac{1}{2}a - \frac{1}{2} - b)_r(1 + a - b)_r} x^{2r}$$

$$\times {}_2F_1\left(\begin{matrix} c + r, 1 + 2b + r \\ 1 + a - c + 2r \end{matrix}; x\right)$$

$${}_4F_3\left(\begin{matrix} a - 2b - 1 + r, \frac{1}{2}a + \frac{1}{2} - b + r, -b - 1 + r, c + r \\ \frac{1}{2}a - \frac{1}{2} - b + r, 1 + a - c + 2r, 1 + a - b + r \end{matrix}; x\right)$$

provided $a - c - e = 2b$.

The basic analogue of (5.7) may be written as below (by using (5.1) for $m = 0$ in (3.5))

$$(5.8)\quad {}_5\Phi_4\left(\begin{matrix} q^a, q^{\frac{1}{2}a+1}, -q^{\frac{1}{2}a+1}, q^b, q^c \\ q^{\frac{1}{2}a}, -q^{\frac{1}{2}a}, q^{1+a-b}, q^{1+a-c} \end{matrix}; x\, q^{a-2b-2c}\right)$$

$$= \sum_{r=0}^{\infty} \frac{(q^{2b-1}; r)(q^{1+a-2c}; r)(q^{a-2b-1}; r)(q^{\frac{1}{2}a+\frac{1}{2}-b}; r)}{(q; r)(q^{a-c+r}; r)(q^{1+a-c}; 2r)(q^{\frac{1}{2}a-\frac{1}{2}-b}; r)}$$

$$\times \frac{(-q^{\frac{1}{2}a+\frac{1}{2}-b}; r)(q^{-b-1}; r)(q^c; r)}{(-q^{\frac{1}{2}a-\frac{1}{2}-b}; r)(q^{1+a-b}; r)} x^{2r} q^{r^2+(c+a-2c)r}$$

$$\times {}_2\Phi_1\left(\begin{matrix} q^{c+r}, q^{2b+1+r} \\ q^{1+a-c+2r} \end{matrix}; x\, q^{a-c}\right)$$

$$\times {}_5\Phi_4\left(\begin{matrix} q^{a-2b-1+r}, q^{\frac{1}{2}a+\frac{1}{2}-b+r}, -q^{\frac{1}{2}a-b+r+\frac{1}{2}}, q^{-b-1+r}, q^{c+r} \\ q^{\frac{1}{2}a-\frac{1}{2}-b+r}, -q^{\frac{1}{2}a-\frac{1}{2}-b+r}, q^{1+a-b+r}, q^{1+a-c+2r} \end{matrix}; xq^{1+a-2c}\right)$$

with $a - c - e = 2b$.

Similar expansions could also be obtained from results due to Shukla (**8**, vii) and Henrici (**5**, $a \sim b$, $a \sim c$).

I am grateful to Dr. R. P. Agarwal for his kind help and guidance during the preparation of this paper.

References

1. N. Agarwal, J. Lond. Math. Soc. *34* (1959), 37–46.
2. W. N. Bailey, *Generalized hypergeometric series* (Cambridge Tract, 1935).
3. ——— J. Lond. Math. Soc., *22* (1947), 237–40.
4. T. W. Chaundy, *Proc. Lond. Math. Soc.* (*2*), *50* (1949), 56–74.
5. P. Henrici, Pacific J. Math., *5* (1955), 923–31.
6. M. Jackson, J. Lond. Math. Soc., *27* (1952), 116–23.
7. F. H. Jackson, Amer. J. Math., *32* (1910), 305–14.
8. H. S. Shukla, Quart. J. Math. (Oxford), *10* (1959), 48–59.

Lucknow University

ON CONNECTIONS BETWEEN GROWTH AND DISTRIBUTION OF ZEROS OF INTEGRAL FUNCTIONS

Q. I. RAHMAN

1. The following theorem was proved by Paley and Wiener (**4**, p. 70; **1**, p. 136).

THEOREM 1. *If $f(z)$ is a canonical product of order 1 with real zeros, and $f(0) = 1$, the conditions*

$$\lim_{r\to\infty} \int_{-r}^{r} x^{-2} \log|f(x)|dx = -\pi^2 A, \tag{1}$$

and

$$\lim_{r\to\infty} r^{-1} n(r) = 2A, \tag{2}$$

are equivalent. $n(r)$ denotes the number of zeros of absolute value not exceeding r.

Instead of assuming the zeros to be all real Pfluger assumed that the zeros are close to the real axis and proved the following theorem (**5** or **1**, p. 143).

THEOREM 2. *Let*

$$f(z) = e^{cz} \prod_{n=1}^{\infty} \left(1 - \frac{z}{z_n}\right) \exp\left(\frac{z}{z_n}\right)$$

be an entire function of exponential type, with $f(0) = 1$. Then the conditions

$$\lim_{r\to\infty} r^{-1} n(r) = D, \qquad \sum_{n=1}^{\infty} r_n^{-1} |\sin \theta_n| = \pi C < \infty \tag{3}$$

and

$$\lim_{r\to\infty} \int_{-r}^{r} x^{-2} \log|f(x)|dx = -\pi^2 I \neq \pm\infty \tag{4}$$

are equivalent, and $D = 2C + 2I$.

For a general order $\rho (0 < \rho < 1)$, the following theorem was proved by Boas (**2**).

THEOREM 3. *If $f(z)$ is of order less than 1, all its zeros are real and negative and $f(0) = 1$, the conditions*

$$\lim_{r\to\infty} r^{-\rho} n(r) = A, \tag{5}$$

Received July 2, 1958. Research supported by the National Science Foundation.

and

$$(6)\quad \int_0^r x^{-1-\sigma}\{\log|f(-x)| - \pi\cot\pi\sigma\cdot n(x)\}dx \sim \pi A(\rho-\sigma)^{-1}(\cot\pi\rho - \cot\pi\sigma)r^{\rho-\sigma}$$

(for any σ, $0 < \sigma < 1$*) are equivalent. When* $\sigma = \rho$, (6) *is to be interpreted as*

$$(6')\quad \int_0^\infty x^{-1-\rho}\{\log|f(-x)| - \pi\cot\pi\rho\cdot n(x)\}dx = -\pi^2 A\operatorname{cosec}^2\pi\rho.$$

In Theorem 4 of this note we extend the result of Boas to the case where the zeros do not necessarily lie on the negative real axis but are close to certain lines.

THEOREM 4. *Let*

$$(7)\quad f(z) = \prod_{n=1}^{\infty}\left(1 - \frac{z}{z_n}\right)$$

be an entire function of order less than 1. *If*

$$(8)\quad \sum_{n=1}^{\infty} r_n^{-\sigma}\{2\sin(\theta_n + \pi)\sigma + \sin 2\pi\sigma\} = C \neq \pm\infty \qquad (0 < \sigma < 1)$$

then the conditions (5) *and*

$$(9)\quad \int_0^r x^{-1-\sigma}\{\log|f(-x)| - \pi\cot\pi\sigma\cdot n(x)\}dx \sim \pi A(\rho-\sigma)^{-1}(\cot\pi\rho - \cot\pi\sigma)r^{\rho-\sigma} + \frac{\pi C}{\sigma(1-\cos 2\pi\sigma)}$$

are equivalent. When $\rho = \sigma$, (9) *is to be interpreted as*

$$(9')\quad \int_0^\infty x^{-1-\rho}\{\log|f(-x)| - \pi\cot\pi\rho\cdot n(x)\}dx = -\pi^2 A\operatorname{cosec}^2\pi\rho + \frac{\pi C}{\rho(1-\cos 2\pi\rho)}.$$

On putting $\rho = \sigma = \frac{1}{2}$ in the above theorem and interpreting the result in terms of functions of order 1, we get Pfluger's theorem. Since (8) is satisfied *a priori* for every $\sigma > \rho$ we have the following

COROLLARY. *If*

$$f(z) = \prod_{n=1}^{\infty}\left(1 - \frac{z}{z_n}\right)$$

is an entire function of order less than 1, *and* $\rho < \sigma < 1$ *then the conditions* (5) *and* (9) *are equivalent.*

Proof of Theorem 4. We prove the theorem by comparing $f(z)$ with another function which has real negative zeros. Let

$$F(z) = \prod_{n=1}^{\infty} \left(1 + \frac{z}{r_n}\right),$$

where $r_n = |z_n|$. We have

$$\log \left| \frac{f(-x)}{F(-x)} \right| = \sum_{n=1}^{\infty} \log \left| \frac{z_n + x}{r_n - x} \right| .$$

The series on the right has non-negative terms and so

$$(10) \quad \int_0^r x^{-1-\sigma} \log|f(-x)|\,dx = \int_0^r x^{-1-\sigma} \log|F(-x)|\,dx + \sum_{n=1}^{\infty} \int_0^r x^{-1-\sigma} \log \left| \frac{z_n + x}{r_n - x} \right| dx.$$

The number of zeros of $F(z)$ in $|z| \leqslant x$ is $n(x, F) \equiv n(x, f) \equiv n(x)$. Subtracting

$$\int_0^r x^{-1-\sigma} \pi \cot \pi\sigma \cdot n(x)\,dx$$

from both sides of (10), we get

$$(11) \quad \int_0^r x^{-1-\sigma} \{\log|f(-x)| - \pi \cot \pi\sigma \cdot n(x)\}\,dx = \int_0^r x^{-1-\sigma} \{\log|F(-x)| - \pi \cot \pi\sigma \cdot n(x)\}\,dx + \sum_{n=1}^{\infty} \int_0^r x^{-1-\sigma} \log \left| \frac{z_n + x}{r_n - x} \right| dx.$$

We now show that, as $r \to \infty$, the limit (finite or infinite) of the sum on the right is

$$(12) \qquad \frac{\pi}{\sigma(1 - \cos 2\pi\sigma)} \sum_{n=1}^{\infty} r_n^{-\sigma} \{2 \sin (\theta_n + \pi)\sigma + \sin 2\pi\sigma\}.$$

To do this put

$$\phi(z) = \log \frac{z_n + z}{r_n - z},$$

where it is assumed that z_n is not real and negative. If the value of z^σ is the principal value and we integrate $z^{-1-\sigma}\phi(z)$ around the contour consisting of the circle $|z| = r$ with a cut from r to 0 and back again having indentations to avoid r_n's and the origin, then $\phi(z)$ increases by $2\pi i$ as we traverse the contour starting at $z = r$. On integration by parts

$$\begin{aligned} \int z^{-1-\sigma} \phi(z)\,dz &= -\frac{2\pi i}{\sigma r^\sigma} + \frac{1}{\sigma} \int z^{-\sigma} \phi'(z)\,dz \\ &= -\frac{2\pi i}{\sigma r^\sigma} + \frac{1}{\sigma} \int z^{-\sigma} \left(\frac{1}{z_n + z} + \frac{1}{r_n - z} \right) dz \\ &= -\frac{2\pi i}{\sigma r^\sigma} + \frac{1}{\sigma} 2\pi i\,(-z_n)^{-\sigma} - \frac{1}{\sigma} \pi i r_n^{-\sigma} (1 + e^{-2\pi i\sigma}) \end{aligned}$$

$$= -\frac{2\pi i}{\sigma r^\sigma} + \frac{2\pi i}{\sigma}\{r_n e^{i(\theta_n+\pi)}\}^{-\sigma} - \frac{1}{\sigma}\pi i r_n^{-\sigma}(1+e^{-2\pi i\sigma})$$

$$= -\frac{2\pi i}{\sigma r^\sigma} + \frac{2\pi i}{\sigma} r_n^{-\sigma} e^{-i(\theta_n+\pi)\sigma} - \frac{1}{\sigma}\pi i r_n^{-\sigma}(1+e^{-2\pi i\sigma}).$$

As $r \to \infty$, the integral along $|z| = r$ tends to zero, so we have (combining the integrals along the two sides of the cut and equating real parts in the limiting form of the equation)

$$(1-\cos 2\pi\sigma)\int_0^\infty x^{-1-\sigma}\log\left|\frac{z_n+x}{r_n-x}\right| dx = \frac{\pi}{\sigma} r_n^{-\sigma}\{2\sin(\theta_n+\pi)\sigma + \sin 2\pi\sigma)\}$$

or

$$\int_0^\infty x^{-1-\sigma}\log\left|\frac{z_n+x}{r_n-x}\right| dx = \frac{\pi}{\sigma(1-\cos 2\pi\sigma)} r_n^{-\sigma}\{2\sin(\theta_n+\pi)\sigma + \sin 2\pi\sigma\}.$$

$F(z)$ has only real negative zeros and $n(r, F) \equiv n(r, f) \sim Ar^\rho$. Therefore (Theorem 3 above) the integral on the right-hand side of (11) is

$$\sim \pi A\,(\rho-\sigma)^{-1}(\cot\pi\rho - \cot\pi\sigma)\, r^{\rho-\sigma}$$

which is to be interpreted for $\sigma = \rho$ as $-\pi^2 A \operatorname{cosec}^2\pi\rho$. Hence if we suppose that (8) and (5) hold, then (9) will hold. The fact that (8) and (9) imply (5) is immediate.

2. The following theorem of the same general nature has been proved by Clunie **(3)**.

THEOREM 5. *Let $f(z)$ be an integral function of genus zero and lower order λ if $0 < \lambda < 1$, which has all but a finite number of its zeros, z_n, in the upper hal, plane. If $Rz_n = o(|z_n|)$ as $n \to \infty$, then the conditions*

$$\lim_{x\to\infty} x^{-\rho}\log|f(x)| = \tfrac{1}{2}\pi A \operatorname{cosec}\tfrac{1}{2}\pi\rho \tag{3}$$

and

$$\lim_{r\to\infty} r^{-\rho} n(r) = A \tag{5}$$

are equivalent.

Let $n_+(r)$ and $n_-(r)$ count, respectively, the zeros in $Im\, z > 0$ and $Im\, z < 0$. Following the method of Clunie we prove the following extension of Theorem 5.

THEOREM 6. *Let $f(z)$ be an integral function of genus zero and lower order λ, $0 < \lambda < 1$. If at least one of the two numbers $n_+(r)$ and $n_-(r)$ is $O(r^\rho)$ as $r \to \infty$ and $Rz_n = o(|z_n|)$ as $n \to \infty$, then (13) implies (5).*

Proof. Let us suppose for definiteness that $n_-(r) = O(r^\rho)$. Without loss of generality we may assume that $f(0) = 1$. Let, consequently,

$$f(z) = \prod_{n=1}^{\infty}\left(1-\frac{z}{z_n}\right) = \prod_{m=1}^{\infty}\left(1-\frac{z}{b_m}\right)\prod_{n=1}^{\infty}\left(1-\frac{z}{c_n}\right) = P(z)\cdot Q(z),$$

where b_m and c_n denote respectively, the zeros lying in the upper half plane and the lower half plane. If δ is fixed, $0 < \delta < \pi$, and $z = re^{i(\pi-\delta)}$ then (3, p. 139) for $m > m_0(\delta)$

$$\left|\frac{b_m - z}{b_m - r}\right| < 1.$$

Hence

$$\left|\frac{P(z)}{P(r)}\right| < \prod_{m=1}^{m_0} \left|\frac{b_m - z}{b_m - r}\right| \to 1$$

as $r \to \infty$, and thus as $r \to \infty$,

$$\log|P(z)| < \log|P(r)| + o(1).$$

Further, if we take δ to be sufficiently small, then, for $n > n_0(\delta)$, we will have

$$\left|\frac{c_n - z}{c_n - r}\right| < 2.$$

Hence

$$\left|\frac{Q(z)}{Q(r)}\right| < \prod_{n=1}^{n_0} \left|\frac{c_n - z}{c_n - r}\right| \cdot 2^{n-(r)},$$

and thus as $r \to \infty$

$$\log|Q(z)| < \log|Q(r)| + O(r^\rho).$$

Therefore on the positive real axis and on the radius $\arg z = \pi - \delta$ we find that

$$\log|f(z)| = O(r^\rho).$$

By the Phragmen-Lindelöf principle it follows that $f(z)$ is of order ρ and mean type. The rest of the argument is the same as that of Clunie (3, pp. 139–40).

In conclusion I wish to thank Professor R. P. Boas, Jr. for his valuable guidance. I am also indebted to the referee for suggesting improvements.

References

1. R. P. Boas, Jr., *Entire functions* (New York, 1954).
2. ——— *Integral functions with negative zeros*, Can. J. Math., *5* (1953), 179–84.
3. J. Clunie, *On a theorem of Noble*, J. Lond. Math. Soc. *32* (1956), 138–44.
4. R. E. A. C. Paley and N. Wiener, *Fourier transforms in the complex domain* (New York, 1934).
5. A. Pfluger, *Ueber gewisse ganze Funktionen vom Exponentialtypus*, Comm. Math. Helvet. *16* (1944), 1–18.

Northwestern University
and
Muslim University, Aligarh

A COSINE FUNCTIONAL EQUATION IN HILBERT SPACE

SVETOZAR KUREPA

Throughout this paper R denotes the set of all real numbers, $m(K)$ the Lebesgue measure of $K \subseteq R$, H a Hilbert space, $L(H)$ the set of all linear continuous mappings of H into H, endowed with the usual structure of a Banach space.

We consider the mapping F of the set R into $L(H)$ such that

$$F(x+y) + F(x-y) = 2F(x)F(y) \tag{1}$$

holds for all $x, y \in R$. In **(2)** we have solved this equation under the assumption that H is of finite dimension. In this paper we prove that a weak measurability of F implies its weak continuity in the case of separable Hilbert space. In Theorem 2 we prove that every weakly continuous solution of (1) in the set of normal transformations has the form $F(x) = \cos(xN)$, where the normal transformation N does not depend on x.

We start with a preliminary lemma.

LEMMA 1. *Let K be a linear Lebesgue measurable set such that $0 < m(K) < +\infty$. There exists a number $a > 0$ with the property that for every $x \in (-a, a)$ there are $s_1(x), s_2(x), s_3(x) \in K$ such that $s_1(x) = s_2(x) - x/2 = s_3(x) - x$.*

Proof. Let $u(x)$ be the function defined on the set of all real numbers R by the equation $u(x) = m(K \cap (K - x/2) \cap (K - x))$. If $\chi(t)$ denotes the characteristic function of the set K then

$$\begin{aligned} |u(x) - u(0)| &= |\int \chi(t)[\chi(t + x/2)\chi(t + x) - \chi(t)\chi(t + x) \\ &\qquad + \chi(t)\chi(t + x) - \chi(t)]dt| \\ &\leqslant \int |\chi(t + x/2) - \chi(t)|dt + \int |\chi(t + x) - \chi(t)|dt. \end{aligned}$$

Since the right side tends to zero as $x \to 0$ we find the function $u(x)$ continuous in $x = 0$. Since $u(0) = m(K) \neq 0$, there exists a constant $a > 0$ such that $u(x) \neq 0$ for all $x \in (-a, a)$. But $u(x) \neq 0$ implies $K \cap (K - x/2) \cap (K - x) \neq \phi$. Hence for each $x \in (-a, a)$ there are $s_1(x), s_2(x), s_3(x) \in K$ such that $s_1(x) = s_2(x) - x/2 = s_3(x) - x$ and hence Lemma 1 is proved.

THEOREM 1. *Let F be a mapping of R into $L(H)$ which satisfies (1) for every $x, y \in R$.*

Suppose that: (1) there is an interval $I = [a, b] \subseteq R$ such that the restriction of F to I is weakly measurable;

Received December 28, 1958. Presented under the same title to the International Congress of Mathematicians, Edinburgh, 1958.

(2) *if* $F(x)f = 0$, *almost everywhere, then* $f = 0$; (3) H *is a separable Hilbert space.*

Then F *is weakly continuous on* R.

Proof. We divide the proof into three parts.

1. The function F is measurable on R. (1) implies:

$$F\left(x - \frac{b-a}{2}\right) = 2F(x)F\left(\frac{b-a}{2}\right) - F\left(x + \frac{b-a}{2}\right).$$

When x runs through the interval $[a, \frac{1}{2}(a+b)]$ then $x + \frac{1}{2}(b-a)$ runs over the interval $[\frac{1}{2}(a+b), b]$. Since $F(y)$ is measurable on each of these intervals we find that $F(y)$ is measurable on the interval $[a - \frac{1}{2}(b-a), a]$. Thus, the measurability of the function F on the interval I implies the measurability of this function on the interval $I' = [a - \frac{1}{2}(b-a), b]$. The way by which I' is obtained from I enables us to deduce that the function F is measurable on the set $(-\infty, b)$. For $x = 0$ (1) implies that F is an even function. Thus the function F is measurable on the set of all real numbers.

2. The function F is locally bounded. The separability of H implies immediately that $x \to ||F(x)||$ is a measurable function, hence there is a measurable set $K \subset R$ of strictly positive measure such that $L = \sup ||F(x)|| < +\infty$, $(x \in K)$. We assert that $||F(x)||$ is bounded on every finite interval. Since the function F is an even function we can, without loss of generality, assume that $K \subseteq [0, +\infty]$. If we put $x + y$ instead of y in (1) we get: $F(x) = 2F(x+y)F(y) - F(x+2y)$. This implies:

$$||F(x)|| \leqslant 2||F(x+y)|| \cdot ||F(y)|| + ||F(x+2y)||. \tag{2}$$

For $x = y$ (1) implies: $F(2x) = 2F^2(x) - E$ and this gives:

$$||F(2x)|| \leqslant 2||F(x)||^2 + 1. \tag{3}$$

From (2) and (3) we get:

$$||F(x)|| \leqslant 2||F(x+y)|| \cdot ||F(y)|| + 2||F(y + \tfrac{1}{2}x)||^2 + 1. \tag{4}$$

According to Lemma 1 there exists a number $a > 0$ with the property that for every $x \in (0, a)$ a number y can be found such that $y, y + \frac{1}{2}x, y + x \in K$. If $x \in (0, a)$ and if y is the corresponding element of K then (4) implies: $||F(x)|| \leqslant 4L^2 + 1$ for every $x \in (0, a)$. Thus the function $||F(x)||$ is bounded on the interval $(0, a)$. This and (3) imply that $||F(x)||$ is bounded on the interval $(0, 2a)$. From this we infer that the function $||F(x)||$ is bounded on every finite interval of the type $(0, b)$, $(b > 0)$. Since F is an even function we have that it is bounded on every finite interval.

3. The function F is weakly continuous. Since the function $F(x)$ is measurable and locally bounded, the functional

(5) $$\int_a^b (F(x)f, g)\,dx$$

is a bounded linear function on H for any $a, b \in R$ and $g \in H$. There is, therefore, a unique element $g_{ab} \in H$ such that:

$$\int_a^b (F(x)f, g)\,dx = (f, g_{ab})$$

for every $f \in H$. Let H' denote the set of all g_{ab}. We assert that H' is dense everywhere on H. In fact, let $h \in H$, $h \perp H'$, that is, let

(6) $$\int_a^b (F(x)h, g)\,dx = 0$$

for all $g \in H$ and for all numbers a and b. For given, but arbitrary g, (6) implies:

(7) $$(F(x)\,h, g) = 0$$

for $x \notin S_g$ where $mS_g = 0$. Let $A = \{g_1, g_2, g_3, \ldots,\}$ be a countable set dense in H and let

$$S = \bigcup_{n=1}^{\infty} S_{g_n}.$$

According to (7) we have

(8) $$(F(x)h, g_n) = 0$$

for all $x \notin S$. Since A is dense in H (8) implies $F(x)h = 0$ for every $x \notin S$, that is, almost everywhere. The requirement of Theorem 1 implies $h = 0$, that is, the set H' is dense in H.

If we put $2F(y)f$ instead of f in (5) and if we use (1) we find:

(9) $$2(F(y)f, g_{ab}) = \int_{a+y}^{b+y} (F(x)f, g)\,dx + \int_{a-y}^{b-y} (F(x)f, g)\,dx.$$

If y_k tends to y_0, then (9) implies: $(F(y_k)f, h) \to (F(y_0)f, h)$ for every $h \in H'$. Since the sequence $F(y_k)f$ is bounded and since H' is dense in H we find

$$(F(y_k)f, g) \to (F(y_0)f, g)$$

for each pair $f, g \in H$, that is, $F(y_k)$ tends weakly to $F(y_0)$ whenever y_k tends to y_0. This proves that F is weakly continuous. Q.e.d.

THEOREM 2. *Let $N(x)$ be a mapping of R into $L(H)$ which satisfies* (1) *for every $x, y \in R$.*

Suppose that: (1) *$N(x)$ is a normal transformation for every $x \in R$;* (2) *if $N(x)f = 0$, almost everywhere, then $f = 0$;* (3) *$N(x)$ is weakly continuous.*

Then a bounded self-adjoint transformation B and self-adjoint transformation A which commutes with B can be found in such a way that

$$N(x) = \tfrac{1}{2}[\exp(ixN) + \exp(-ixN)] = \cos(xN)$$

holds for all x where $N = A + iB$.

Proof. I. As in Theorem 1 we have

$$\int_a^b (N(x)f, g)\,dx = (f, g_{ab}).$$

We assert that the set H' of all g_{ab} is dense in H. In fact if h is an element of H which is orthogonal on H', then (6) holds for all $a, b \in R$ and $g \in H$. The continuity of function $(N(x)f, g)$ together with (6) imply (7) for every $x \in R$ and for every $g \in H$. From here we get $N(x)h = 0$ for all x which implies $h = 0$. Thus the set H' is dense in H. Using (1) we obtain:

$$\left(\frac{N(x) - E}{x} f, g_{ab}\right) = \frac{1}{2x}\left[\int_b^{b+x} (N(u)f, g)\,du + \int_b^{b-x} (N(u)f, g)\,du - \int_a^{a+x} (N(u)f, g)\,du - \int_a^{a-x} (N(u)f, g)\,du\right]$$

which implies:

$$\lim_{x\to 0}\left(\frac{N(x) - E}{x} f, g_{ab}\right) = 0$$

for every $g_{ab} \in H'$ and for every $f \in H$. From here it follows that the sequence

$$\frac{N^*(x) - E}{x} h$$

converges weakly to zero for every $h \in H'$, when $x \to 0$. There exists, therefore, a number $M(h)$ such that:

$$\|[N(2^{-n}) - E]\,h\| \leqslant 2^{-n} M(h).$$

This implies that the series

$$\sum_{n=1}^{\infty} \|[N(2^{-n}) - E]h\|^2 \tag{10}$$

is convergent for every $h \in H'$.

II. The fact that $N(x)$ is an even function implies that $N(x)$ and $N(y)$ commute one with another for every couple of real numbers x and y. Now we consider the functional equation (1) only for x and y from the set

$$G = \{r | r = 2^{-l}k,\ l, k = 0, \pm 1, \pm 2, \ldots,\}.$$

Since G is countable and since $N(r)$ and $N(r')$ $(r, r' \in G)$ commute we find **(4**, p. 67**)**,

$$N(r) = \int_R f(\xi, r) E(\Delta_\xi) \tag{11}$$

where $E(\Delta)$ is a real spectral measure and the function $f(\xi, r)$ is $E(\Delta)$-measurable and finite everywhere for every $r \in G$. If we put (11) in (1) we get:

$$f(\xi, r + r') + f(\xi, r' - r) = 2f(\xi, r)f(\xi, r') \tag{12}$$

for all $r, r' \in G$ and for almost all ξ (G is countable!). Using (11) we can write (12) in the form:

$$\lim_{n\to\infty} \int_R \sum_{k=1}^{n} |f(\xi, 2^{-n}) - 1|^2 ||E(\Delta_\xi)h||^2.$$

From the above it follows that the series

$$\sum_{n=1}^{\infty} |f(\xi, 2^{-n}) - 1|^2 \tag{13}$$

is convergent almost everywhere with respect to the measure $||E(\Delta)h||^2$. Since the set H' is dense in H the series (13) is convergent almost everywhere with respect to $E(\Delta)$. Thus

$$f(\xi, 2^{-n}) \to 1 \tag{14}$$

almost everywhere with respect to $E(\Delta)$. It follows from (14) and (12) that

$$f(\xi, r) = \tfrac{1}{2}[\exp irf(\xi) + \exp(-irf(\xi))] \tag{15}$$

hold true almost everywhere in ξ and for all $r \in G$ (see **(2**, Lemma 4**)**). Here $\phi(\xi)$ is $E(\Delta)$-measurable and everywhere finite complex-valued function. Thus the transformations

$$N = \int_R \phi(\xi)E(\Delta_\xi), A = \int_R [Re\phi(\xi)]E(\Delta_\xi) \text{ and } B = \int_R [Im\phi(\xi)]E(\Delta_\xi) \tag{16}$$

are defined. Since

$$||N(r)|| = \operatorname{ess\,sup} |f(\xi, r)| < +\infty$$

for every $r \in G$, we find:

$$\operatorname{ess\,sup} |\operatorname{Im} \phi(\xi)| < +\infty,$$

that is, the transformation B is bounded. Then (16), (15), and (11) imply:

$$N(r) = \tfrac{1}{2}[\exp(irN) + \exp(-irN)] = \cos(rN)$$

for every $r \in G$. By the weak continuity and the fact that the set G is dense on R we find: $N(x) = \cos(xN)$ for every $x \in R$.

Remark 1. If we consider a mapping $r \to N(r)$ of the set G in the set $L(H)$ such that:

(1) $N(r)$ is a normal transformation;

(2) $N(r + r') + N(r' - r) = 2N(r)N(r')$ for all $r, r' \in G$, and

(3) $\lim ||N(1/2^n) - E|| = 0$

then $N(r) = \cos(rN)$, where normal transformation N does not depend on r. Indeed the representation (11) holds in this case too. Since $||N(r)|| = \operatorname{ess\,sup} |f(\xi, r)|$ (14) also holds. This together with (11) leads to (12) and consequently to (15), from which $N(r) = \cos(rN)$ follows.

References

1. R. Phillips and E. Hille, *Functional analysis and semigroups*, Amer. Math. Sci. Coll. Pub. (1957).
2. S. Kurepa, *A cosine functional equation in n-dimensional vector space*, Glasnik mat. fiz. i astr., *13* (1958), 169–189.
3. ——— *On the (C)-property of functions*, Glasnik mat. fiz. i astr., *13* (1958), 33–38.
4. B. Sz. Nagy, *Spektraldarstellung Linearer Transformationen des Hilberschen Raumes* (Berlin, 1942).

Department of Mathematics, Zagreb

SHEETS OF REAL ANALYTIC VARIETIES

ANDREW H. WALLACE

Introduction. In a previous paper **(4)** the author worked out some results on the analytic connectivity properties of real algebraic varieties, that is to say, properties associated with the joining of points of the variety by analytic arcs lying on the variety. It is natural to ask whether these properties can be carried over to analytic varieties, since the proofs in the algebraic case depend mainly on local properties. But although this generalization can be carried out to a large extent, there are, nevertheless, difficulties in the analytic case, owing mainly to the fact (cf. **2**, § 11) that a real analytic variety may not be definable by means of a set of global equations. Thus, although the general idea of the treatment given here is the same as in **(4)**, some variation in the details of the method has proved to be necessary, and some of the final results are slightly weaker in form.

As in **(4)** the key result is an approximation theorem for piecewise analytic curves on a variety; this theorem is stated in § 2 and then proved in §§ 3 and 4. In § 5 the approximation theorem is applied to the discussion of the sheets, that is, the maximal analytically connected sets, of a real analytic variety.

As regards further literature on the subject of real analytic varieties, see Whitney **(5** and **6)**; in the former paper an approximation theorem of the type just mentioned is proved for analytic manifolds (that is, varieties without singularities), while in the latter certain decomposition theorems are obtained for a wide class of varieties.

1. Real analytic varieties. In this paper the term real analytic variety will be applied to a set V in a fixed Euclidean space E_n such that V is closed in E_n and each point p of V has a neighbourhood U in the ambient space such that $U \cap V$ is the set of zeros of a finite collection of functions analytic in U. Thus the term is equivalent to "sous-ensemble analytique" as in **(2)**. At each point p of V, V defines a germ of a real analytic variety V_p. Write V_p' for the complexification of V_p, that is to say, the smallest germ of a complex analytic variety containing V_p and contained in the complex n-space obtained by allowing the co-ordinates in E_n to take complex values. The dimension of V_p' (that is to say, the dimension of the highest dimensional component of V_p') will be called the local dimension of V at p, to be written as $\dim_p V$. $\mathrm{Dim}_p V$ has a maximum ($< n$) over all points p of V; this maximum will be called $\dim V$.

Received November 3, 1958.

A regular or simple point of V is a point p at which $\dim_p V = \dim V$ and at which local analytic co-ordinates can be set up in E_n in such a way that V has locally the equations $x_{r+1} = x_{r+2} = \ldots = x_n = 0$. A singular point of V is a point which is not regular; note that this includes any point where the local dimension is less than the maximum for V. The set of all singular points of V will be called the singular locus of V.

It is essential at this point to note that the singular locus of a real analytic variety is not necessarily an analytic variety. For example, consider the analytic variety defined in E_3 by the single equation $x^2y^2 - z^2(y + z) = 0$. The cross-section of this surface by a plane $y =$ constant is a cubic curve with a loop, and as y tends to zero this loop flattens out into the line segment on the x-axis joining the points $x = \pm 2/3\sqrt{3}$. It is then easy to check that the singular locus of this variety consists of this line segment along with the whole y-axis, and this set is certainly not an analytic variety. Of course the surface under consideration could be regarded as a real algebraic variety, in which case the whole of the x-axis would be included in the singular locus, and this locus would be an algebraic sub-variety. The essential difference is that for real analytic varieties the regularity or otherwise of a point is determined by local equations, and not, as in the algebraic case, by global equations (which in general do not exist in the analytic case; cf. **(2)**).

Another feature of the example just given concerns the approximation of analytic arcs (definition at the beginning of § 2) on the surface V with the equation $x^2y^2 - z^2(y + z) = 0$. Take two regular points of V on the x-axis and on opposite sides of the origin, say the points $(\pm 1, 0, 0)$, and call them p and q. The segment pq of the x-axis is an analytic arc joining p and q but there is no other arc joining these points in such a direct manner. In fact if C is any other arc on V joining p and q and if K is its projection on the (x, y)-plane, then the part of K lying in the strip defined by $|x| \leqslant 2/3\sqrt{3}$ is covered three times by part of C. It follows, for example, from this that an approximation of K, however good, cannot be lifted to an approximation of C in V in the manner of **(4)**. The trouble is that in **(4)** the success of the method used depended on the fact that the arcs studied never had more than finitely many points in common with the singular locus of the variety. But, as can be seen from the present example, an arc on a real analytic variety can have a sub-arc in common with the singular locus, even when the end-points are regular.

The example just given indicates that, in order to study properties of real analytic varieties analogous to those studied in **(4)** for algebraic varieties, a weaker form of approximation for curves will have to be used, in which the approximation C' of a given curve C will lie in a preassigned neighbourhood of C, but C' will be mapped on C by a mapping which may be (at least along certain arcs) many-one.

2. Statement of the approximation theroem. For convenience some

of the definitions of **(4)** will be repeated here. An analytic arc in Euclidean n-space E_n is an arc given by parametric equations $x_i = f_i(t)$, $i = 1, 2, \ldots, n$, where the f_i are real analytic functions of t. The end-points of such an arc are assumed to be non-singular; that is to say, the given equations define a simple linear branch at each end-point. A piecewise analytic curve is a union of finitely many analytic arcs joined end to end, in such a way that at a common end-point P of two of the arcs, say C_1 and C_2, exactly these two arcs meet and no others, and C_1 and C_2 have distinct tangents at P. Each point P of the type described is called a joint of the curve. A curve C' is said to be an ϵ-approximation of a curve C if there is a homeomorphism f of C' on C such that the distance of p from $f(p)$ is less than ϵ for each p. C' and C are said to be analytically equivalent at p if $f(p) = p$, and if, in a sufficiently small neighbourhood U of p, there is defined a mapping T of the form $T(x_i) = x_i + h_i(x)$, where the h_i are real analytic functions of $x_1, x_2, \ldots, x_n$ at p, such that $T(C \cap U) = C' \cap U$. Here the h_i, expanded in power series at p, are assumed to be of order $\geqslant 2$; if they are of order $\geqslant r$, the analytic equivalence is said to be of order $\geqslant r$.

One of the main results of **(4)**, which will be required here is:

LEMMA 2.1. *Let C be a piecewise analytic curve in E_n and let S be a finite set of points on C including all singular points of C (note that the joints of C are not to be counted as singularities of C). Then for any preassigned ϵ and r there is an analytic curve C' which is an ϵ-approximation of C with analytic equivalence of order $\geqslant r$ at each point of S.*

For any set A in E_n the ϵ-neighbourhood of A is the set of points in the union of all spheres of radius ϵ with centres at the points of A. With this terminology the approximation theorem to be proved in this paper can be stated.

THEOREM 1. *Let V be a real analytic variety in E_n and let C be a piecewise analytic curve on V, all the joints of C being regular on V. Then for any preassigned ϵ there is an analytic arc C' on V and contained in the ϵ-neighbourhood of C. In particular the end-points of C' are within ϵ-neighbourhoods of those of C, and if C is closed so is C'.*

The idea of the proof of this theorem is as follows. If $\dim V = r$, C will be projected on a suitable r-dimensional linear subspace E_r of E_n. Writing the projected curve as K, Lemma 2.1 will be applied to give an approximation K' of K. K' is then to be lifted into V. In the case of a real algebraic variety V (or more generally a real analytic variety given by global equations, with singular points defined globally as in algebraic geometry), this lifting is in general carried out by a one-one correspondence, yielding the stronger approximation theorem of **(4)**. Here, however, the lifting has to be done by means of the local equations of V, splitting K' into a sequence of arcs for the purpose, and lifting each one in turn. The lifted arcs are then to be strung together to

give the required curve C'. As illustrated in the example of § 1 the sequence of lifted arcs may double back on itself covering parts of K' several times. It has to be checked of course that C' cannot break up into closed loops, or the last condition to be proved in the theorem would not hold.

Most of the proof is taken up with the process of choosing a set of co-ordinates so that the projection just referred to is the orthogonal projection onto the space $x_{r+1} = x_{r+2} = \ldots = x_n = 0$. The method is to take a point p on C, and using local equations for V in a neighbourhood $U(p)$ of p, to make a list of the various conditions unfavourable to the projection, approximation and lifting process described above. It turns out that, if co-ordinates are to be changed by orthogonal transformations, then the choices which are unfavourable, in $U(p)$, correspond to an analytic subvariety in the space of orthogonal transformations. Since the curve C can be contained in a finite number of neighbourhoods of the type $U(p)$ it follows that a choice of co-ordinates can be made which is favourable for the whole of C.

3. Choice of co-ordinates. The procedure sketched at the end of the last section will now be carried out in detail. Take a point p of V as origin. In a neighbourhood $U(p)$ of p, V is defined as the set of zeros of a finite number of power series in $x_1, x_2, \ldots, x_n$ with real coefficients, convergent in $U(p)$. Alternatively, V is the set of real zeros of an ideal I in the ring of power series in $x_1, x_2, \ldots, x_n$ with real coefficients convergent near p. Write V' for the complexification of V at p, that is to say, the smallest complex analytic variety, defined in a complex neighbourhood $U'(p)$ of p (obtained by allowing all the co-ordinates to assume complex values) whose set of real points coincides with $V \cap U(p)$. If I is the ideal of V at p then the ideal of V' is generated by I in the ring of power series with complex coefficients convergent around p.

Take an irreducible component V_0 of $V \cap U(p)$ with $\dim V_0 = \dim V$, provided such a component exists. In the applications to follow this choice will always be possible; but to cover the contrary case, if $\dim_p V \neq \dim V$, no restriction will be imposed on the choice of co-ordinates around p. The co-ordinates are now to be changed in such a way that the prime ideal of V_0 at p becomes a regular ideal **(1**, p. 208**)**. This means that, in the new co-ordinates $y_1, y_2, \ldots, y_n$, the ideal is to contain no power series independent of y_{r+1}, $y_{r+2}, \ldots, y_n$ but for each $h > r$ it must contain a power series regular with respect to y_h, that is to say, having an exact power of y_h among its terms of lowest order. The method of regularizing an ideal is explained in **(1**, p. 208, Theorem 4**)**. It involves a sequence of linear changes of co-ordinates, which can in fact be taken to be orthogonal. And at each stage the condition that a change of co-ordinates should not be suitable is that the elements of the corresponding matrix should satisfy certain algebraic equations. However, the procedure followed in **(1)** is not quite suitable for the present purpose. For there the discussion is carried out in terms of formal series, after which a check has to be made as to the region of convergence. This region may

well depend on the particular choice of co-ordinates made, whereas here it is necessary to work in a sequence of steps, making sure that at each there is a region of convergence independent of the co-ordinates chosen. The following is a variant of the method of **(1)** designed to meet this requirement.

LEMMA 3.1. *Let C be a compact set of the real analytic variety V. Then co-ordinates can be chosen, making an orthogonal linear transformation from those originally given, such that, in a neighbourhood of each point p of C the co-ordinates of points on V satisfy a polynomial equation in x_n with coefficients analytic in $x_1, x_2, \ldots, x_{n-1}$ at p.*

Proof. The set C used here will eventually be an analytic curve on V, but for the moment compactness is the only property wanted. Let $p \in C$, and for convenience shift the origin of the given co-ordinates $x_1, x_2, \ldots, x_n$ in E_n to p. In a neighbourhood $U(p)$ of p the points of V are the zeros of an ideal I in the ring of power series in the x_i with real coefficients convergent around p. Take a series f in I and assume $U(p)$ is such that f is convergent in $U(p)$. Let A be a generic orthogonal $n \times n$ matrix and define the co-ordinates y_i by $y_i = \sum_{j=1}^{n} a_{ij}x_j$. Clearly there is an algebraic subvariety $W(p)$ of the set O_n of orthogonal $n \times n$ matrices such that any specialization of A not in $W(p)$ will give a set of co-ordinates $y_1, \ldots, y_n$ such that f is regular with respect to y_n. Now, by the Weierstrass preparation theorem, f can be multiplied by a power series in the y_i, not vanishing at p, to give a polynomial g in y_n whose highest coefficient is 1 and whose other coefficients all are power series in $y_1, y_2, \ldots, y_{n-1}$ vanishing at p. Now the proof of the Weierstrass preparation theorem **(1)** shows that all the series involved in the theorem are convergent in a smaller neighbourhood $U'(p)$ than $U(p)$, obtained in fact by reducing the bounds of the various co-ordinates by a factor which depends on the upper bound of f in $U(p)$. Bearing in mind that the linear change of co-ordinates being made here is orthogonal, thus leaving spheres invariant, it follows that if $U(p)$ is taken as a spherical neighbourhood, $U'(p)$ can be taken as a smaller sphere whose radius is a fraction of that of $U(p)$. The fraction depends on the upper bound of f in $U(p)$, but does not depend on the particular choice of the orthogonal matrix A. C, being compact, can be covered by a finite number of neighbourhoods of the type $U'(p)$, and so the union of the corresponding $W(p)$ makes up an algebraic subvariety of the set O_n. If the matrix A changing the co-ordinates from the x_i to the y_j is chosen not in this subvariety it follows at once that the conditions of the lemma are satisfied by the new co-ordinates.

Note that, as the conclusion of the lemma has been left, it is not necessarily true that the polynomial in y corresponding to some point p of C has its coefficients vanishing at p, unless p happens to be one of the finite set of points corresponding to the finite set of $U'(p)$ covering C. However some factor of this polynomial will satisfy this condition if the origin is shifted so that $y_n = 0$ at p. On the other hand, even without taking any further steps

beyond the proof described above, the polynomial in y_n corresponding to any point of C will always have the coefficient of the highest power of y_n equal to 1.

The choice of co-ordinates made in the last lemma is to fix y_n once and for all, subsequent changes affecting only the co-ordinates, $y_1, y_2, \ldots, y_{n-1}$. With the choice of co-ordinates just described, let p be any point of C, and repeat the argument of Lemma 3.1, replacing the ideal I of that lemma by the intersection of I with the ring of real analytic functions at p independent of y_n. This argument shows that, for points of V in a neighbourhood of each point of C, y_{n-1} satisfies a polynomial equation with coefficients analytic in $y_1, y_2, \ldots, y_{n-2}$ at p, in particular the coefficient of the highest power of y_{n-1} being 1. Proceeding in this way step by step, the following result is obtained:

LEMMA 3.2. *With the assumptions of the last lemma, there ia a choice of co-ordinates $x_1, x_2, \ldots, x_n$ in E_n such that in some neighbourhood of each point p of C, the co-ordinates of points on V satisfy a set of equations of the form:*

$$f_i(x_1, x_2, \ldots, x_{r+i}) = 0, i = 1, 2, \ldots, n - r, \tag{1}$$

where f_i is a polynomial in x_{r+i} with coefficients real analytic in $x_1, x_2, x_3, \ldots, x_{r+i-1}$ at p, the coefficient of the highest power of x_{r+i} being 1.

It is to be understood in this statement that the set of f_i may change when the point p is changed. On the other hand, in the case which is to be considered later, it will be true that $\dim_p V = \dim V$ at each point p of C, and this will be precisely the value of r for each set of equations of the type (1).

A further adjustment to the co-ordinate system is necessary to enable the local equations of V to be brought into a certain canonical form. Let p be a point of V at which $\dim_p V = \dim V = r$, and let V_0 be an r-dimensional component of V in a neighbourhood of p. Taking p as origin let R_n denote the ring of power series in $x_1, x_2, \ldots, x_n$ with real coefficients convergent around p and let I be the ideal of V_0 in this ring. In the residue class ring R_n/I let ξ_i be the residue class of x_i, for each i. Then equations (1) are satisfied with $(x_1, x_2, \ldots, x_n)$ replaced by $(\xi_1, \xi_2, \ldots, \xi_n)$, from which it follows at once that the quotient field of R_n/I is a finite algebraic extension of that of R_r, the ring of convergent power series in $\xi_1, \xi_2, \ldots, \xi_r$ with real coefficients. In addition, the dimensional condition imposed at p implies that the ξ_i for $i = 1, 2, \ldots, r$ are independent indeterminates over the real numbers. The object of the next bit of working is to pick out a primitive root for this extension, and then to change the co-ordinates so that this root will be the residue class of one of the co-ordinates. That this can be done locally at the point p is, of course, a well-known result. But here the idea is to make the choice of co-ordinates in such a way as to bear the relation just described to each component of V in some neighbourhood of each point of a compact subset C.

Returning now to the notation just introduced, note that the ξ_{r+i} for $i = 1, 2, \ldots, n - r$ are integral over R_r. Let $u_1, u_2, \ldots, u_{n-r}$ be independent

indeterminates over the quotient field of R_r and write $R_r' = R_r[u_1, u_2, \ldots, u_{n-r}]$. Then clearly

$$\xi = \sum_{i=1}^{n-r} u_i \xi_{r+i}$$

is integral over R_r'. Thus ξ will satisfy an equation of the type:

$$\xi^m + a_1 \xi^{m-1} + \ldots + a_m = 0, \tag{2}$$

where each of the a_i is in R_r'. As regards the convergence conditions, each of the a_i is a polynomial in the u_j with coefficients in R_r, and so only finitely many power series are involved in the equation (2), each series being convergent for sufficiently small values of the ξ_i. (That these series are convergent at all can be seen, for example, from the fact that equation (2) can be derived by rational processes from equations satisfied by the individual ξ_{r+i}, $i = 1, 2, \ldots, n-r$, such as the equations (1), where convergence is known. Note that so far nothing is said or known about the reducibility or otherwise of (2).) Now the theorem of the primitive root for a finite algebraic extension **(3)** says that, provided the u_i do not satisfy a set of linear equations (which they do not, being independent indeterminates), ξ is a primitive root for the quotient field of $R_r'(\xi_{r+1}, \xi_{r+2}, \ldots, \xi_n)$. This means in particular that

$$\xi_i = F_i(u, \xi_1, \xi_2, \ldots, \xi_r, \xi)/G(u, \xi_1, \xi_2, \ldots, \xi_r) \tag{3}$$

for each $i = 1, 2, \ldots, n-r$, where each F_i is a polynomial in the u_j and ξ, with coefficients in R_r, and G is a polynomial in the u_j with coefficients in R_r. Then in all the equations (3) there are only finitely many power series in $\xi_1, \xi_2, \ldots, \xi_r$, all convergent for sufficiently small values of the ξ_i. Identifying ξ_i with x_i for each $i = 1, 2, \ldots, r$, it follows that there is a neighbourhood $U(p)$ of p in which all the series (in $x_1, x_2, \ldots, x_r$) appearing in the equations (2) and (3) are convergent. Also denote by $L(p)$ the set of linear equations in the u_i which must not be satisfied if ξ is to be a primitive root as just described. Then if C is a compact set on V it can be covered by a finite number of neighbourhoods of the type $U(p)$, and the u_i can be given real values such that none of the corresponding sets of equations $L(p)$ are satisfied, and such that the rational functions appearing in the equations of the type (3) corresponding to each of these neighbourhoods are defined. At least one of the u_i will be non-zero, say u_1. Then take as a new set of co-ordinates in E_n

$$x_1, x_2, \ldots, x_r, \sum_{i=1}^{n-r} u_i x_{r+i}, x_{r+2}, \ldots, x_n.$$

Changing the notation so that these co-ordinates are again written as $x_1, x_2, \ldots, x_n$ the result obtained can be summed up as follows:

LEMMA 3.3. *Let C be a compact subset of the real analytic variety V such that, at each point p of C, $\dim_p V = \dim V = r$. Then co-ordinates in E_n can be chosen in such a way that C is covered by a finite number of neighbourhoods in each of*

which the points of each r-dimensional local component of V satisfy equations of the form

$$F(x_{r+1}) = 0 \tag{4}$$
$$x_i = F_i(x_{r+1})/G, \qquad i = 2, \ldots, n-r,$$

where F and the F_i are polynomials in x_{r+1} with coefficients which are power series in $x_1, x_2, \ldots, x_r$, and G is a power series in $x_1, x_2, \ldots, x_r$, all the series being convergent in the relevant neighbourhood.

(It is assumed in speaking of these power series that the origin has been shifted to a certain point of the neighbourhood in question.)

Finally take any point p on the compact set C as origin. p will lie in some neighbourhood of the covering of C described in the last lemma, and so the points of the r-dimensional components of V at p will satisfy equations of the type (4), with G and the coefficients of the F_i and of F real analytic at p. The irreducible factors of F corresponding to these components can now be picked out, and will have coefficients which can be written as power series in $x_1, x_2, \ldots, x_r$ convergent in some neighbourhood of p; the co-ordinates $x_{r+2}, x_{r+3}, \ldots, x_n$ for points of these components will still be given by (4), convergence of the series involved holding in some neighbourhood of p. These remarks enable a refinement of Lemma 3.3. to be stated:

LEMMA 3.4. *C being as in the last lemma each point p of C has a neighbourhood $U(p)$ in which each r-dimensional component of V is exactly the set of points satisfying equations of the type* (4) *with F and the F_i polynomials in x_{r+1} and (with p as origin) G and the coefficients of F and the F_i power series in $x_1, x_2, \ldots, x_r$ convergent in $U(p)$. In addition, C, being compact, can be covered by a finite number of neighbourhoods of the type $U(p)$.*

At this stage it is convenient to make a definition in preparation for the next section. In the notation of the last lemma, cover C by a finite number of the neighbourhoods $U(p)$, and set up equations of the type (4) for each r-dimensional component of V in each such neighbourhood. Let D be the discriminant of F; it will be a series convergent in $U(p)$. Then the set of points in $(x_1, x_2, \ldots, x_r)$-space defined by $G = D = 0$ is a local analytic variety in the projection of $U(p)$. The union of all the local varieties obtained in this way from all the r-dimensional local components of V in all the $U(p)$ of the finite covering of C described in Lemma 3.4. will be called the branch locus of V relative to the sets of local equations described in that lemma (or simply branch locus if the context is clear). For brevity a set of points in a Euclidean space which, like the branch locus just introduced, in the union of a finite number of local analytic varieties, each defined in some neighbourhood, will be called an open variety.

4. Displacement of an arc from an open variety. As already pointed out, one of the difficulties presented by real analytic varieties is that a curve,

although not lying entirely in the singular locus, may nevertheless have an arc in common with that locus. The lemma about to be proved is the main step towards resolving this difficulty.

LEMMA 4.1. *Let V be an open variety in Euclidean n-space E_n, and let C be an analytic arc contained in V. Then there exists in E_n an analytic arc C', which is an arbitrarily good approximation of C and which meets V only at finitely many points.*

Proof. Clearly no generality is lost by assuming that all the components of the various local analytic varieties of which V is composed are of dimension $n-1$; this can always be arranged if necessary by enlarging V. The discussion of the last section can now be applied to V. The argument is not affected by the fact that V is now an open variety rather than a real analytic variety, since at each stage only local properties are used. It then follows that co-ordinates can be chosen in such a way that C is covered by a finite number of neighbourhoods in each of which V is given by equations of the type (4). In this case these equations reduce to a single polynomial equation in x_n with coefficients which are power series in the remaining variables convergent in the neighbourhood in question, a point in that neighbourhood being taken as origin. Let the parametric equations of C be $x_i = f_i(t)$, $i = 1, 2, \ldots, n$, where the f_i are real analytic functions of t, and t varies over some finite interval, say $0 \leqslant t \leqslant 1$. Then there is an analytic mapping of the (t, x_n)-plane into E_n given by $f(t, x_n) = (f_1(t), f_2(t), \ldots, f_{n-1}(t), x_n)$. The image of f in E_n is a piece of analytic surface S containing C, and in particular C is the image of the curve $\bar{C}$ in the (t, x_n)-plane with the equation $x_n = f_n(t)$. If $F(x_1, x_2, \ldots, x_n) = 0$ is the equation defining one of the local varieties of which V is composed, then the equation

$$F(f_1(t), f_2(t), \ldots, f_{n-1}(t), x_n) = 0$$

defines a local variety in a neighbourhood of some point of the (t, x_n)-plane, and the union of all the local varieties obtained in this way forms an open variety in this plane. Denote this variety by $\bar{V}$. It is clear that the image of $\bar{V}$ under f is the intersection of S and V, and, moreover, the points of $\bar{V}$ are the only ones mapped into $S \cap V$. And so if the lemma can be proved for the curve $\bar{C}$ relative to the open variety $\bar{V}$ in the (t, x_n)-plane, giving an approximation $\bar{C}'$ of $\bar{C}$ meeting $\bar{V}$ at only finitely many points, then the curve $C' = f(\bar{C}')$ will satisfy the requirements of the lemma. In order to prove the lemma in the plane it is clearly sufficient to take $\bar{C}'$ to be any sufficiently good approximation of $\bar{C}$ in the plane. But in view of the applications to be made of this result, it is necessary to make the approximation in a particular way, as will now be explained. The open variety $\bar{V}$ consists of a finite number of curve branches, each defined in some neighbourhood; let the finite collection of points p_i denote the centres of these branches along with a finite set of points arbitrarily chosen on $\bar{C}$. Let t_i be the value of t at p_i. Let $g(t)$ be a polynomial in t vanishing only at the t_i, to an order at least r. For example

$g(t) = \Pi(t - t_i)^r$ will do. Then, remembering that $\bar{C}$ has the equation $x_n = f_n(t)$ define $\bar{C}'$ as the curve with equation $x_n = f_n(t) + \lambda g(t)$, where λ is a real parameter. Note that, in a neighbourhood of each p_i the power series expressions of the parametric equation of $\bar{C}$ and of $\bar{C}'$ differ only by high power of the parameter if r is taken large, and also that, as the parameter λ tends to zero, the approximation of $\bar{C}$ by $\bar{C}'$ can be made arbitrarily close. Since one of the branches making up $\bar{V}$ at each p_i is part of $\bar{C}$, and since $\bar{C}$ and $\bar{C}'$ meet only at the p_i, it is not hard to see that, for λ samll enough, $\bar{C}'$ will meet $\bar{V}$ only at the p_i. Applying the mapping f to the curve $\bar{C}'$ constructed in this way, the following corollary of the above lemma is obtained:

COROLLARY. *In the above lemma, C' can be constructed in such a way that, at each of the finitely many points where it meets V, each of its branches is associated with a branch of C, and, with a suitable choice of parameter, the parametric equations of these branches differ only by terms of high order with coefficients depending analytically on a parameter λ and tending to zero as λ tends to zero.*

The proof of Theorem 1 can now be undertaken, the following lemma giving the discussion of the most difficult step in the proof.

LEMMA 4.2. *Let V be a real analytic variety in E_n and let C be an analytic arc on V with at least one of its end-points regular on V. Let C_0 be the set of points on C for which the local dimension of V is $r = \dim V$, and let co-ordinates be chosen in E_n in accordance with Lemma 3.4, relative to the compact set C_0 on V. Let B be the branch locus in $(x_1, x_2, \ldots, x_r)$-space E_r corresponding to this co-ordinate choice, and to the choice of local equations for V around a finite number of points of C_0. Then in the ϵ-neighbourhood of C on V, for preassigned ϵ, there is an analytic arc C' whose projection in E_r meets B at only finitely many points. And in particular the end-points of C' will lie in ϵ-neighbourhoods of those of C.*

Proof. Let K be the projection of C in E_r. If $K \cap B$ already consists of finitely many points there is nothing to be done, for C' can be taken equal to C. But it may be that subarcs of K lie in B. In this case a set of points p_i is to be defined on C, along with their projections q_i on K (the q_i being not necessarily all distinct). The q_i are to include all singularities of K and all isolated points of $K \cap B$, and the p_i are to include all points of C projecting on these. Using local equations of the type (4) for V in neighbourhoods of a finite number of points of C, it may turn out that certain arcs on K can be lifted to give several copies on V, apart from those which form part of C. The p_i are to include the intersections of C with these other copies (these points will clearly be finite in number) and the q_i are to include their projections. Finally, approximate K by an arc K' in E_r as in Lemma 4.1 and its corollary. According to these results $K' \cap B$ consists of finitely many points, and it is clear from the proof of the corollary that these can be assumed to include the q_i already defined. Any additional intersections of K' and B are now to

be included also among the q_t, and as before all points of C projecting on them are to be taken among the p_t. It will be remembered that according to the corollary to Lemma 4.1, K' depends on a parameter λ and that, around the q_t, K' takes the limiting position K as λ tends to zero. It is now to be shown that, if the approximation of K by K' is close enough and if λ is small enough there is an arc C' on V satisfying the requirements of this lemma and projecting on K'.

To establish the existence of this arc C', sets of neighbourhoods covering C and K will now be constructed. K' will then be made to lie in the union of these neighbourhoods, and will be divided into arcs each lying in one of the neighbourhoods. These arcs will then be lifted into V, and it will be shown that some of them can be joined end to end to form the required analytic arc C'. First define $U(q_t)$ as a neighbourhood of q_t such that the parametric equations of each branch of K' at q_t, when expressed in terms of a suitable parameter, give each co-ordinate as a power series convergent in $U(q_t)$, and in fact uniformly convergent with respect to λ, and also such that, if these equations are substituted into the equations of the type (4) for V around p_t, the resulting equations can be solved for $x_{r+1}, x_{r+2}, \ldots, x_n$ as fractional power series in the parameter, convergent for values of the parameter corresponding to points of K' in $U(q_t)$. If several q_t coincide, take $U(q_t)$ as the smallest of the corresponding neighbourhoods. $U(p_t)$ is then to be a neighbourhood of p_t projecting onto $U(q_t)$. In addition $U(p_t)$ is assumed to be taken so small that no two curve branches on V at p_t projecting into branches of K' at q_t have any point in common other than p_t. It should be noted that, as the results of § 3 are being used here, what has just been said makes sense only around the points of C_0 and their projections. It will appear presently, however, that $C = C_0$. The curves C, K, K' will now be split up into a number of arcs for which it is convenient to introduce some terminology now. These arcs will be called C-arcs, K-arcs, or K'-arcs according to the curve they lie on. C-arcs lying in the neighbourhoods $U(p_t)$ will be said to be of the first kind. When these arcs are removed the remainder of C consists of finitely many disjoint non-singular arcs. Those whose projections are contained in B will be said to be of the second kind, and those whose projections do not meet B of the third kind. There is a certain amount of arbitrariness in the definition of B, depending as it does in the choice of particular neighbourhoods; it is not hard to see that, by shrinking certain of these neigbourhoods if necessary, it can be arranged that the whole of C is a union of arcs of the three kinds described. The projections of these arcs will be called K-arcs of the first, second, and third kinds, respectively.

Construct now an open covering of C by sets in V. Let γ be a C-arc of the second or third kind, and let κ be its projection in E_r. Let $U(\gamma)$ be a neighbourhood of γ not meeting C except in the points of an arc obtained by extending γ slightly in each direction (not far enough to reach any of the p_t). Also $U(\gamma)$ is to be chosen so that its projection $U(\kappa)$ meets K in the

arc κ slightly extended at each end. The set of $U(p_i)$ and $U(\gamma)$ covers C while the $U(q_i)$ and $U(\kappa)$ cover K. Now in each $U(q_i)$ there will be a set of branches of K' approximating K-arcs of the first kind, and if the approximation of K by K' is sufficiently close each $U(\kappa)$ will contain exactly one non-singular arc of K' approximating κ. These arcs of K' lying in the $U(q_i)$ and the $U(\kappa)$ will be called K'-arcs of the first, second, or third kind according to the kind of K-arc they approximate.

C'-arcs, some of which will make up the required curve C', will now be defined. To obtain a C'-arc of the first kind, take a K'-arc κ' of the first kind, through q_i, say, and change the parameter on it so that it is zero at q_i. Substitute these parametric equations into the appropriate equations of the type (4) for V, and calculate all the corresponding roots x_{r+1} as fractional power series in the parameter t. By the choice of the $U(p_i)$ and $U(q_i)$ convergence holds for these series for all t corresponding to points on κ', and the resulting curve branches in E_n will all actually lie in $U(p_i)$. If the fractional power series corresponding to one of these branches involve an even root of t, the end-points of that branch will lie in the same set $U(\gamma)$ for some γ whenever the parameter λ on which K' depends is taken small enough. On the other hand, if an odd root of t is taken, the end-points of the branch will lie in two different $U(\gamma)$'s for λ small enough. The set of all branches on V obtained in this way will be called C'-arcs of the first kind. Consider now a K'-arc κ' of the second kind approximating a K-arc κ. κ' is to be lifted into V in a similar way to that applied to the arcs of the first kind. κ' in this case may pass through several neighbourhoods in each of which a different set of equations of the type (4) for V must be used, and so κ' must be lifted in sections. A number of copies will be obtained of κ' lifted in this way into V, and, taking κ' to be a compact arc, it is clear that the points of certain of the lifted arcs will converge to the points of some C-arc lying over κ, as the parameter λ on which K' depends tends to zero, and the convergence is uniform with respect to the variable point on κ'. If γ' is one of these lifted arcs, converging to the arc γ as λ tends to zero, γ' will lie in $U(\gamma)$ for λ sufficiently small. Assume now that λ is so small that this happens for all arcs like γ' obtained in this way; these arcs will be called C-arcs of the second kind. C'-arcs of the third kind are obtained in the same way from the K'-arcs of the third kind. The only difference is that in this case there is a unique C'-arc over a given K'-arc.

Suppose that the family of C'-arcs has been constructed and that λ is so small that the conditions mentioned relative to the arcs of the second and third kinds and the end-points of those of the first kind are satisfied. A maximal C'-arc can now be defined as a maximal union of C'-arcs which is itself an analytic arc. Since two distinct analytic arcs cannot have a subarc in common, it is clear that each C'-arc belongs to exactly one maximal arc, and also the C'-arcs forming a maximal arc follow one another in a well-defined sequence (defined by the variation of an analytic parameter on the maximal arc) in which each C'-arc is traced out exactly once, unless the maximal arc is closed.

Now one end-point p of C is assumed, in the hypothesis of the lemma, to be regular on V. If γ_1 is the C-arc on which p lies, it follows that there is exactly one C'-arc γ_1' which has γ_1 as its limit when λ tends to zero, and exactly one point p' of that arc will have p as limit. The last statement rules out the possibility that γ_1' is an arc of the first kind with parameter obtained from that of γ_1 by taking an even root. Now define C' to be the unique maximal C'-arc starting off with γ_1'. C' is certainly not closed, for it has p' as an end-point. The other end of γ_1' will be joined to a second C'-arc γ_2', that to a third γ_3', and so on until the other end of C' is reached. This must happen after a finite number of steps, since there are only finitely many C'-arcs, no one of which can be used twice. Also, it has been arranged that each C'-arc of the second or third kinds will lie in one of the $U(\gamma)$ and so can be assumed to end in one of the $U(p_i)$, so that it will join up to an arc of the first kind; and similarly each C'-arc of the first kind will join up to one of the second or third kind; all this with the exception of arcs which end near the end-points of C. It follows that the second end-point of C' will lie in a preassigned neighbourhood of the second end-point of C, if λ is small enough. Also, the definition of the C'-arcs has ensured that, if λ is small enough, C' will lie in a preassigned neighbourhood of C, and so the requirements of the lemma are satisfied by C', whose projection K' meets B at only finitely many points.

COROLLARY. *With the notations of the last lemma, C_0, the set of points on C where the local dimension of V is $r = \dim V$, coincides with C.*

Proof. The proof of this is implicit in what has gone before. If the result is not true there will be a point p_0 different from the initial point p of C such that at all points of the arc pp_0 the local dimension of V is r, but following p_0 and arbitrarily close to it there will be points of lower local dimension. p_0 will in this case necessarily be among the points p_i defined above. Let γ be the C-arc which passes beyond p_0 into the region of lower local dimension, κ its projection, and κ' the K'-arc which approximates it. Then every C'-arc lying in $U(p_0)$ over κ' must correspond to taking an even root of the parameter on κ', since the second half of κ' has no points of V over it near p_0. It would follow that C' could not have a second end-point; for such an end-point could not lie over any point of K' preceding q_0, and yet it follows from what has just been said that a moving point on C', starting at p, must always double back when it reaches p_0, always projecting on a point of K' which precedes q_0. But since there are only finitely many C'-arcs and C' cannot be closed a contradiction is thus obtained which proves the corollary.

The proof of Theorem 1 will now be completed. C is now to be a piece-wise analytic curve on V with all the joints at regular points of V. Co-ordinates in E_n are to be chosen as in Lemma 3.4, the curve C being taken as the compact set; this choice of compact set is admissible in view of the corollary of the last lemma which shows that the local dimension of V is r at all points

of C. Apply Lemma 4.2 to each of the analytic arcs of which C is composed. The result is a collection of analytic arcs $\bar{C}_t$ lying in a preassigned neighbourhood of C, with end-points lying arbitrarily close to the end-points and joints of C, and with projections in E_r meeting the branch locus B in finitely many points. In addition, since the joints of C are regular on V, it can be assumed that the end-points of the $\bar{C}_t$ lie in cellular neighbourhoods of these points, and so they can be joined up by analytic arcs within these cells. And these new analytic arcs will have projections in E_r not meeting B. Thus, given the piecewise analytic curve C, a new piecewise analytic curve $\bar{C}$ has been constructed in a preassigned neighbourhood of C, with its end-points in preassigned neighbourhoods of those of C, and such that the projection K of $\bar{C}$ in E_r meets the branch locus B in at most finitely many points. Thus to complete the proof of Theorem 1 it is only necessary to prove the theorem for $\bar{C}$. And the major difficulty has now been removed, namely that caused by subarcs of the given curve projecting into the branch locus. Using Theorem 3 of **(4)**, quoted above as Lemma 2.1, let K' be an approximation of K, with analytic equivalence at all singularities of K and at points of $K \cap B$, but smoothing K at the joints. In addition, the results leading to Theorem 3 of **(4)** imply that K' can be assumed to depend on a parameter λ in such a way that, as λ tends to zero, K' takes the limiting position K in a neighbourhood of each of the singularities and points of $K \cap B$. K' is now to be lifted into V to give the analytic curve C' required by Theorem 1. The simplest way of doing this is to repeat the argument of Lemma 4.2, with the simplification here that there are no arcs of the second kind. Alternatively the lifting can be done as in **(4)**, using sets of local equations like (4) for V instead of the global equation which was available here. Note that if this second method is used, it is possible to make C' and $\bar{C}$ analytically equivalent at the singularities of the latter. This may be of interest if $\bar{C}$ happens to be the curve which is given. However if the given curve is such that the initial adjustment replacing C by $\bar{C}$ (to avoid having arcs projecting into B) it necessary, any property of analytic equivalence is liable to be lost in the process. It is not hard to see that this adjustment will be necessary if and only if C has arcs in common with the singular locus of V, a situation which has been shown to be possible by the example of § 1.

One further remark must be made concerning Theorem 1. It will be noticed that the approximating curve C' given by that theorem passes through all the points p_t constructed in the course of the proof of Lemma 4.2, and that along with the points which must belong to this set any finite collection of points on C can be included. This can be stated as a corollary which strengthens the result of the theorem:

COROLLARY 2. *In Theorem* 1, *C' can be constructed so as to pass through each of a finite set of points arbitrarily given on C. In particular the end-points of C' can be made to coincide with those of C.*

5. Sheets of an analytic variety. Let V be a real analytic variety in E_n. A subset S of V is said to be analytically connected if every pair of points of S can be joined by an analytic arc lying in S. A sheet of V is an analytically connected subset not contained in any larger analytically connected subset of V. The sheet S is said to be proper if it contains a point p with a neighbourhood U in E_n such that $V \cap U = S \cap U$. This terminology agrees with that of **(4)**. The following results correspond to some of the properties derived for sheets of real algebraic varieties in **(4)**.

LEMMA 5.1. *Let p, q, r be three points of a real analytic variety V and let q be regular on V. Then, if there are analytic arcs on V joining p to q and joining q to r, there is an analytic arc on V joining p to r and meeting a preassigned neighbourhood of q.*

Proof. The proof is as for Lemma 17.1 of **(4)**, using here Theorem 1 and its Corollary 2 to approximate the union of the given arcs pq and qr by an analytic arc from p to r.

THEOREM 2. *Let p be a regular point of the real analytic variety V and let S be the set of all points of V which can be joined to p by analytic arcs on V. Then S is a sheet of V, and every sheet of V containing a regular point can be constructed in this way.*

Proof. The proof, using Lemma 5.1, is essentially the same as that of Theorem 13 of **(4)**.

The following two corollaries correspond similarly to the corollaries of Theorem 13 in **(4)**.

COROLLARY 1. *Each regular point of V belongs to exactly one sheet.*

COROLLARY 2. *Each sheet of V containing a regular point of V is proper.*

The next theorem corresponds to the dimensional homogeneity established in **(4)** for sheets of real algebraic varieties:

THEOREM 3. *Let S be a sheet of a real analytic variety V containing a regular point p of V. Then for any q on S, every neighbourhood of q contains a point q' of S which is regular on V.*

Proof. Let C be an analytic arc joining p and q. Set up a co-ordinate system as for Lemma 4.2 relative to C, and apply that lemma, along with the Corollary 2 at the end of § 4. This gives an analytic arc C' joining p and q and with its projection K' in E_r meeting the branch locus B in only finitely many points. In particular, C' itself can meet the singular locus of V in at most finitely many points, and so any neighbourhood of q must contain a regular point q' of V lying on C'. Since q' is joined to the regular point p by an analytic arc on V, Theorem 2 along with its first corollary implies that q' is on S as required.

A sheet S containing a regular point of V will be called r-dimensional. The local cellular decomposition described in § 18 of **(4)** carries over to the real analytic case, since the whole construction depends only on the setting up of local equations. The result is:

LEMMA 5.2. *Let p be a point of a real analytic variety of dimension r and let W be a subvariety containing p (W in fact need only be defined in a neighbourhood of p). Then in any preassigned neighbourhood of p there is a neighbourhood U of p such that $V \cap U$ is the union of the closures of a set of disjoint open cells U_i of dimensions $\leqslant r$ such that:*

(1) $\cup \operatorname{Fr} U_i = U \cap W'$ *where W' is an analytic subvariety of V, defined at least around p, such that $U \cap W' \supset U \cap W$.*

(2) *Each r-cell in the decomposition of $V \cap U$ is contained in exactly one proper sheet (note that here, unlike the algebraic case, this statement is only made for the cells of highest dimension).*

(3) $p \in \bar{U}_i$ *for each i.*

(4) *The neighbourhood U of p can be chosen so that all points of $U \cap (V - W)$ can be joined to p by analytic arcs on V meeting W only at p.*

To make the statement of part (2) of the above lemma complete, note that each s-cell (for $s \leqslant r$) in the decomposition described there consists of regular points of a real analytic variety of dimension s defined in a neighbourhood of p. Such a cell is thus analytically connected, and so is contained in a maximal analytically connected subset of V, namely a sheet. But a sufficiently small neighbourhood of a point of the cell in question will meet V only at points of the cell, and so the sheet so obtained is proper. A slight strengthening of this statement gives the following theorem:

THEOREM 4. *Every point of a real analytic variety V belongs to a proper sheet of V.*

Proof. Take any point p on V, and construct a cellular decomposition of V around p as in Lemma 5.2. Let M be one of the cells, say of dimension $s \leqslant r$. As already pointed out, M is analytically connected. And so, by part (4) of Lemma 5.2, the set consisting of M along with the point p is analytically connected, and so is contained in some sheet. But a small neighbourhood of a point of M meets V only at points of M, and so this sheet is proper.

It is worth noting that, in the notation of this theorem, the closure $\bar{M}$ of the cell M is analytically connected. For M is part of a real analytic variety V_0 defined at least in a neighbourhood of p. Now take two points q_1 and q_2 in $\bar{M}$. If they are in M then they certainly be can joined by an analytic arc in $\bar{M}$. Suppose $q_1 \in \operatorname{Fr} M$. Then, applying Lemma 5.2 to V_0 around q_1, it follows that q_1 can be joined by an analytic arc γ_1 in $\bar{M}$ to a point q_2 of M, and if $q_2 \in M$ then q_2 and q_2 can be joined by an analytic arc γ_2 in M. Then, applying Lemma 5.1 to V_0 (the fact that V_0 may be only locally defined

makes no difference), it follows that the union of γ_1 and γ_2 can be replaced by an analytic arc in $\bar{M}$ joining q_1 and q_2. A similar argument can be used if both q_1 and q_2 are in $\mathrm{Fr}M$.

The following result corresponds to Theorem 14 of **(4)**; note, however, the restriction as to dimension.

THEOREM 5. *Let V be a real analytic variety in E_n of dimension r. Then each r-dimensional sheet of V is a closed set.*

Proof. Let S be an r-dimensional sheet of V, and let p be in the closure S of S. Then a neighbourhood U of p contains a point q of S, which, by Theorem 3, can be assumed to be regular on V. By part (4) of Lemma 5.2 if U is small enough p and q can be joined by an analytic arc on V, and so by Theorem 2 and its Corollary 1, p belongs to the unique sheet determined by the regular point q, namely S. S is thus closed.

In contrast to the algebraic case, the properties of the lower dimensional sheets of a real analytic variety are somewhat elusive. For although such sheets are contained in the singular locus of V, this locus may not be an analytic variety. On the other hand, the points of V at which the local dimension is less than the maximum form a subset of the singular locus and this subset is (as will be shown in a future paper) part of a real analytic subvariety. Consequently, the results proved above will all extend to the proper sheets of V, regardless of their dimension. The proposed proof of the assertion just made depends on attaching some sort of multiplicity to each singular point of V. This is done with reference to local systems of equations. Then, attempting to build up a variety of singular points, one fits the p-fold locus in one neighbourhood to the q-fold locus in an adjoining one, with p not necessarily equal to q. p and q are necessarily both even or both odd, and the process only breaks down if one of them is equal to 1. This cannot happen if one has started at a point of lower local dimension, where the multiplicity attached is always even.

REFERENCES

1. S. Bochner and W. T. Martin, *Several complex variables* (Princeton, 1946).
2. H. Cartan, *Variétés analytiques réelles et variétés analytiques complexes*, Bull. Soc. Math. France, *85* (1957) 77–99.
3. B. L. van der Waerden, *Moderne algebra* (Berlin, 1931).
4. A. H. Wallace, *Algebraic approximation of curves*, Can. J. Math. *10* (1958), 242–278.
5. H. Whitney, *Analytic coordinate systems and arcs in a manifold*, Ann. Math., *38* (1937), 809–818.
6. H. Whitney and F. Bruhat, *Quelques propriétés fondamentales des ensembles analytiques-réels*, Comm. Math. Helvet., *33* (1959) 132–160.

University of Toronto

ON FINITE NILPOTENT GROUPS

G. BACHMAN

1. Introduction and notations. It is well known that if $(n, \phi(n)) = 1$, where $\phi(n)$ denotes the Euler ϕ-function, then the only group of order n is the cyclic group. This is a special case of a more general result due to Dickson (**2**, p. 201); namely, if

$$n = p_1^{\alpha_1} \dots p_s^{\alpha_s}$$

where the p_i are distinct primes and each $\alpha_i > 0$, the necessary and sufficient conditions that the only groups of order n are abelian are (1) each $\alpha_i \leqslant 2$ and (2) no

$$p_i^{\alpha_i} - 1$$

is divisible by any $p_1, \dots, p_s$.

We wish to establish a theorem which includes these two results. We let $G(n)$ equal the number of groups of order n where

$$n = \prod_{i=1}^{s} p_i^{\alpha_i},$$

and we seek necessary and sufficient conditions on n so that

$$G(n) = \prod_{i=1}^{s} G(p_i^{\alpha_i}).$$

Clearly, this problem is equivalent to finding necessary and sufficient conditions on n so that all existing groups of order n be nilpotent.

It will be shown that the following is true:

THEOREM 1. *Let*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s},$$

where $p_1, \dots, p_s$ are distinct primes and each $\alpha_i > 0$. The necessary and sufficient conditions that the only groups of order n be nilpotent are: no p_i, $i = 1, \dots, s$, shall divide any

$$p_j^{\alpha_j} - 1, p_j^{\alpha_j - 1} - 1, \dots, p_j - 1, j = 1, \dots, s.$$

We introduce the following notations: the centre of a group A by $Z(A)$, the group of all automorphisms of A by $\Phi(A)$, the group of all inner automorphisms of A by $\Phi'(A)$, the factor group $\Phi(A)|\Phi'(A)$ by $\mathfrak{A}(A)$, the direct

Received November 17, 1958. The author wishes to express his appreciation to Professor H. N. Shapiro for suggesting this problem to him.

product of the two groups A and B by $A \times B$, and the direct product of the n groups $A_1, \ldots, A_n$ by

$$\overset{n}{\underset{i=1}{\times}} A_i,$$

the order of the finite group A by $|A|$, and a Sylow p-group of a group G by S_p.

Let B be a group such that each element $\alpha \in B$ is associated with an automorphism $a \to a^\alpha$ of A. Let G be an extension of A by B, that is, A is a normal subgroup of G and $G|A \simeq B$. Then the elements of G can be written as $g_\alpha a$ where the g_α are in one-to-one correspondence with the $\alpha \in B$, and $a \in A$; also

$$g_\alpha a \cdot g_\beta b = g_{\alpha\beta} f(\alpha, \beta) a^\beta b$$

where $f(\alpha, \beta)$ is a factor system. Moreover,

$$g_\alpha^{-1} a\, g_\alpha = a^\alpha,$$

and

$$(a^\alpha)^\beta = (a^{\alpha\beta})^{f(\alpha,\beta)}.$$

Finally, to the extension G there corresponds a well-defined homomorphism θ of B into $\mathfrak{A}(A)$ **(3**, pp. 121–126**)**. If N is a normal subgroup of G whose order is prime to its index, then G splits over N (Schur's theorem) **(4**, p. 132**)**.

In general, if A is abelian, then $\mathfrak{A}(A) = \Phi(A)$ and B is a group of operators for A, that is, A is a B-module. It is well known that the second cohomology group $H^2(B, A)$ is the group of all group extensions of A by B. If A and B are finite and $(|B|, |A|) = 1$, then $H^r(B, A) = 0$ for all r **(1**, p. 237**)**, in particular, $H^2(B, A) = 0$, so the only extensions of A by B are splitting extensions, that is, we can take $f(\alpha, \beta) = 1$, and, therefore, G contains a subgroup $B' \simeq B$ such that $A \cap B' = e$, the identity element, and $G = AB'$.

The consideration of non-abelian groups A is reduced to the abelian case by the following theorem: There exists a one-to-one correspondence between all non-equivalent extensions of A by B associated with θ and all non-equivalent extensions of $Z(A)$ by the group of operators B corresponding to the homomorphism θ **(3**, pp. 142-145**)**.

In the case of an abelian group A, the non-equivalent splitting extensions of A by B are in one-to-one correspondence with the distinct homomorphisms of B into $\Phi(A)$ **(3**, p. 149**)**. The kernel of the homomorphism will be denoted by W. If $W = B$, then we say that B acts trivially on A.

2. Proof of Theorem 1. (1) *Sufficiency*: To proceed by induction, we assume that the statement is true for every

$$n' = p_1^{\beta_1} \ldots p_s^{\beta_s}, \beta_i \leqslant \alpha_i, n' < n.$$

Now since

$$(|G|, (p_i^{\alpha_i} - 1)(p_i^{\alpha_i - 1} - 1) \ldots (p_i - 1)) = 1,$$

we have, by Frobenius' Theorem **(4**, p. 143**)**, that the maximal p_i-factor group of G is isomorphic to every Sylow p_i-group of G, that is, G contains a normal subgroup N such that $G/N \simeq S_{p_i}$, and G is a splitting extension of N. But there exists a one-to-one correspondence between all non-equivalent extensions of N by S_{p_i} associated with θ and all non-equivalent extensions of $Z(N)$ by the group of operators S_{p_i} corresponding to the homomorphism θ. Thus we must consider splitting extensions, H, of the S_{p_i}-module $Z(N)$. By the induction hypothesis,

$$N = \mathop{\times}_{\substack{j=1 \\ j\neq i}}^{s} S_{p_j}, \qquad \text{so} \qquad Z(N) = \mathop{\times}_{\substack{j=1 \\ j\neq i}}^{s} Z(S_{p_j}).$$

$Z(S_{p_j})$ is an abelian group of order $p_j^{\gamma_j}$, $1 \leqslant \gamma_j \leqslant \alpha_j$, from which it follows **(4**, p. 112**)** that $|\Phi(Z(N))|$ is a divisor of

$$\prod_{\substack{j=1 \\ j\neq i}}^{s} (p_j^{\gamma_j} - 1)(p_j^{\gamma_j} - p_j) \ldots (p_j^{\gamma_j} - p_j^{\gamma_j - 1});$$

whence it is clear that we can only take $W = S_{p_i}$, which means trivial action, that is, the only extension of $Z(N)$ by S_{p_i} is $S_{p_i} \times Z(N)$. Therefore, by the one-to-one correspondence there is only one extension of N by S_{p_i} associated with a given homomorphism θ. Thus, the non-equivalent extensions of N by S_{p_i} are in one-to-one correspondence with those homomorphisms of S_{p_i} into $\mathfrak{A}(N)$ which are associated with extensions of N by S_{p_i}. But

$$\Phi(N) = \mathop{\times}_{\substack{j=1 \\ j\neq i}}^{s} \Phi(S_{p_j}) \qquad \text{and} \qquad |\Phi(N)|$$

is a divisor of

$$\prod_{\substack{j=1 \\ j\neq i}}^{s} (p_j^{\alpha_j} - 1)(p_j^{\alpha_j} - p_j) \ldots (p_j^{\alpha_j} - p_j^{\alpha_j - 1}).$$

Hence $|\mathfrak{A}(N)|$ is also a divisor of this number. Therefore, it is clear that the only possible homomorphism is the trivial one which implies that the only extension of N by S_{p_i} is $S_{p_i} \times N$. But

$$N = \mathop{\times}_{\substack{j=1 \\ j\neq i}}^{s} S_{p_j};$$

hence

$$G = \mathop{\times}_{j=1}^{s} S_{p_j},$$

and G is nilpotent.

(2) *Necessity*: Suppose some

$$p_i/(p_j^{\alpha_j} - 1) \ldots (p_j - 1).$$

Then we consider the following arrangement. Let

$$A(\alpha_j, p_j) = C_{p_j} \times C_{p_j} \times \ldots \times C_{p_j} \qquad (\alpha_j \text{ times})$$

where C_{p_j} is the cyclic group of order p_j. We denote by $G(\alpha_i, p_i)$ a group of order $p_i^{\alpha_i}$. Now, clearly,

$$\Phi\left(\mathop{\times}_{\substack{j=1\\ j\neq i}}^{s} A(\alpha_j, p_j)\right) = \mathop{\times}_{\substack{j=1\\ j\neq i}}^{s} \Phi(A(\alpha_j, p_j)).$$

Since, by assumption,

$$\mathop{\times}_{\substack{j=1\\ j\neq i}}^{s} \Phi(A(\alpha_j, p_j))$$

contains a subgroup of order p_i, there exists a homomorphism:

$$G(\alpha_i, p_i) \to \Phi\left(\mathop{\times}_{\substack{j=1\\ j\neq i}}^{s} A(\alpha_j, p_j)\right)$$

with kernel a normal subgroup W of order $p_i^{\alpha_i - 1}$. Associated with this homomorphism, there is a splitting extension G of

$$\mathop{\times}_{\substack{j=1\\ j\neq i}}^{s} A(\alpha_j, p_j) \qquad \text{by } G(\alpha_i, p_i)$$

for which W is the normal subgroup of $G(\alpha_i, p_i)$ which acts trivially on

$$\mathop{\times}_{\substack{j=1\\ j\neq i}}^{s} A(\alpha_j, p_j).$$

G is, of course, a group of order

$$n = \prod_{i=1}^{s} p_i^{\alpha_i},$$

but the extension G is not equivalent to

$$G(\alpha_i, p_i) \times \left(\mathop{\times}_{\substack{j=1\\ j\neq i}}^{s} A(\alpha_j, p_j)\right).$$

In fact, G is not isomorphic to this group for $S_{p_i} = G(\alpha_i, p_i)$ is not normal in G. Namely, if $a^{-1}g_\alpha a = g_\beta$ then $g_\alpha{}^{-1}a^{-1}g_\alpha a = g_\alpha{}^{-1}g_\beta$, that is, $(a^{-1})^\alpha a = g_\alpha{}^{-1}g_\beta$, but the left side belongs to

$$\mathop{\times}_{\substack{j=1\\ j\neq i}}^{s} A(\alpha_j, p_j)$$

while the right side belongs to S_{p_i}. However,

$$S_{p_i} \cap \left(\mathop{\times}_{\substack{j=1\\ j\neq i}}^{s} A(\alpha_j, p_j)\right) = e,$$

so $g_\beta = g_\alpha$. Now if S_{p_i} were normal in G, then we would have $a^{-1}g_\alpha a = g_\alpha$ for all $g_\alpha \in S_{p_i}$ and all

$$a \in \mathop{\times}_{\substack{j=1\\ j\neq i}}^{s} A(\alpha_j, p_j),$$

that is $(a^{-1})^{\alpha} = a^{-1}$ for all α and all a, which implies that S_{p_i} acts trivially on

$$\mathop{\times}_{\substack{j=1 \\ j\neq i}}^{s} A(\alpha_j, p_j), \quad \text{or} \quad W = S_{p_i},$$

which is a contradiction.

Therefore, S_{p_i} is not normal in G; hence G, of order n, is not nilpotent.

COROLLARY 1. *Let $G(n)$ be the number of groups of order n. If*

$$n = \prod_{i=1}^{s} p_i^{\alpha_i},$$

then the necessary and sufficient conditions in order that

$$G(n) = \prod_{i=1}^{s} G(p_i^{\alpha_i})$$

are that no p_i, $i = 1, 2, \ldots, s$, divides any

$$(p_j^{\alpha_j} - 1)(p_j^{\alpha_j - 1} - 1) \ldots (p_j - 1).$$

Proof. There are $G(p_i^{\alpha_i})$ groups of order $p_i^{\alpha_i}$. By taking all possible direct products it is clear that

$$G(n) \geqslant \prod_{i=1}^{s} G(p_i^{\alpha_i}),$$

and we have equality, if and only if the only groups of order n are direct products of their Sylow subgroups.

It is clear that to have only abelian groups of order n, we must have $\alpha_j \leqslant 2$ for all j; hence we get Dickson's theorem as a special case of Theorem 1.

REFERENCES

1. H. Cartan and S. Eilenberg, *Homological algebra* (Princeton, 1956).
2. L. E. Dickson, Trans. Amer. Math. Soc. *6* (1905), 201.
3. A. G. Kurosh, *The theory of groups*, vol. II (New York, 1956).
4. H. Zassenhaus, *The theory of groups* (New York, 1949).

Rutgers University

FINITE GROUPS WHICH ADMIT AN AUTOMORPHISM WITH FEW ORBITS

DANIEL GORENSTEIN

1. Introduction. In the course of investigating the structure of finite groups which have a representation in the form ABA, for suitable subgroups A and B, we have been forced to study groups G which admit an automorphism ϕ such that every element of G lies in at least one of the orbits under ϕ of the elements g, $g\phi^r(g)$, $g\phi^r(g)\phi^{2r}(g)$, $g\phi^r(g)\phi^{2r}(g)\phi^{3r}(g)$, etc., where g is a fixed element of G and r is a fixed integer.

In a previous paper on ABA-groups written jointly with I. N. Herstein **(4)**, we have treated the special case $r = 0$ (in which case every element of G can be expressed in the form $\phi^i(g^j)$), and have shown that if the orders of ϕ and g are relatively prime, then G is either Abelian or the direct product of an Abelian group of odd order and the quaternion group of order 8. In another paper **(3)**, the author has shown that if each element of G lies in exactly one of these orbits, then G must be an elementary Abelian group of type $(p, p, \ldots, p)$. The purpose of this paper is to prove more generally that any finite group G which admits an automorphism whose orbits are of the above form is necessarily solvable (Theorem 5). The burden of the proof rests on the case in which ϕ leaves only the identity element of G fixed, and in this case we shall show that G is in fact nilpotent (Theorem 4).

In the course of the proof we first establish the nilpotency of G in the so-called non-exceptional case (in particular, if G is solvable) (Theorem 1). For this case our statement and argument resemble a result of Feit **(2)** and Higman **(5)**, which asserts that a solvable group having an automorphism of prime order which leaves only the identity element fixed is necessarily nilpotent.* Their argument actually applies if G is assumed to be p-normal for all $p|o(G)$. Recently it has been announced by J. G. Thompson that G must in fact be p-normal for all $p|o(G)$ whenever G admits an automorphism of prime order leaving only the identity element of G fixed, from which it follows that an arbitrary group G admitting such an automorphism is necessarily nilpotent.†

However, not much is known concerning the structure of G if ϕ is of composite order. It is not difficult to construct a solvable non-nilpotent group G admitting an automorphism ϕ of composite order leaving only the identity

Received October 22, 1958.

*Feit proves the nilpotency of G under the weaker hypothesis that no subgroup of G has an exceptional group as a composition factor.

†A.M.S. Notices, *5* (6) (November, 1958), 695.

element of G fixed; and it is an open question whether G must be solvable to admit such an automorphism even when ϕ has order 4.

We see then that our assumption on the orbits of G is a strong one since no other conditions on G or the order of ϕ are needed to prove that G is nilpotent if ϕ leaves only the identity element of G fixed. A direct consequence of this assumption is a simple inequality (Lemma 2.3) which exists between the order of ϕ and the order of G; and it is this inequality which lies at the heart of many of our arguments.

In §§ 10 and 11 we shall determine the structure of groups of prime power order which admit an automorphism ϕ without non-trivial fixed elements satisfying our special condition on orbits, and shall show that such a group is either Abelian or of class 2 (Theorem 8). Combining this result with Theorem 4, it will follow that any group G admitting such an automorphism ϕ without non-trivial fixed elements is either Abelian or nilpotent of class 2 (Theorem 9).

In the final section we shall determine the precise connection between groups whose orbits satisfy this condition and groups of the form ABA. As an application we shall prove the solvability of a certain class of ABA-groups (Theorem 10).

The author wishes to thank Prof. Herstein for his considerable help in the preparation of this paper, particularly with the proof of Lemma 3.1.

2. ϕ-groups. We shall call a group G a ϕ-group if G admits an automorphism ϕ such that every element of G can be expressed in the form $\phi^i(g\phi^r(g)\dots\phi^{r(j-1)}(g))$ for some fixed integer r and some fixed element g in G, i and j being arbitrary. The element g will be called a *generator* of G under ϕ, and r will be called the *index* of G with respect to g, or simply the index of G.

For simplicity we exclude the trivial case in which the order h of ϕ is 1. This implies, in particular, that $o(G) > 1$. We may further assume that $r|h$ for otherwise set $r_1 = (r, h)$ and define $\phi_1 = \phi^{r/r_1}$. Then clearly ϕ_1 has order h, G is a ϕ_1-group of index r_1 with respect to g, and we have $r_1|h$. In the special case in which $h = r$, and hence in which every element of G can be expressed in the form $\phi^i(g^j)$, we shall say that G is a ϕ-group *of index* 0.

We can imbed G as a normal subgroup of a group G^*, which contains an element a of order h such that $aga^{-1} = \phi(g)$ for all g in G and such that $G^* = GA$, where A denotes the subgroup generated by a. If ϕ is of prime order and leaves only the identity element of G fixed, it is easy to show that G^* is a Frobenius group and that G is the regular subgroup of G^*. By analogy with this case, we shall say, whenever ϕ leaves only the identity element of G fixed, that G is a *regular* ϕ-group, and that ϕ is a *Frobenius* automorphism of G.

For brevity we also introduce the symbol $[g]_r{}^j$ for the element $g\phi^r(g)\dots\phi^{r(j-1)}(g)$. For completeness we set $[g]_r{}^0 = 1$. This symbol has several formal properties which we shall use repeatedly throughout the ensuing discussion, and which for convenience we incorporate into the following lemma:

LEMMA 2.1. *Let ϕ be an automorphism ofo rder h of a group G. For any g in G and any integers i, j, k, r, we have $[[g]_r^j]_{r,i}^k = [g]_r^{jk}$ and $[g]_r^{j+k} = [g]_r^j \phi^{rj}([g]_r^k)$. Furthermore, if $h|r$, $[g]_r^j = g^j$; while if $r|h$ and ϕ^r is Frobenius, $[g]_r^{h/r} = 1$.*

Proof. All these relations except the last follow immediately from the definition of the symbol $[g]_r^j$. On the other hand, if ϕ^r leaves only the identity element of G fixed, it is easy to see that g can be written in the form $x^{-1}\phi^r(x)$ for some x in G. But then $[g]_r^{h/r} = (x^{-1}\phi^r(x))(\phi^r(x^{-1}\phi^r(x)) \dots \phi^{h-r}(x^{-1}\phi^r(x))$ $= x^{-1}\phi^h(x) = 1$.

The following lemma shows that the property of being a ϕ-group carries over to subgroups and factor groups of G.

LEMMA 2.2. *Let G be a ϕ-group of index r with respect to the generator g, and let H be a subgroup of G invariant under ϕ. Then H is a ϕ-group of index rs with respect to the generator $[g]_r^s$ for some integer s. If H is normal in G and $\bar{G} = G/H$ then $\bar{G}$ is a $\bar{\phi}$-group of index r with respect to the generator $\bar{g}$, where $\bar{\phi}, \bar{g}$ denote respectively the image of ϕ on $\bar{G}$ and the residue of g in $\bar{G}$. Furthermore, no proper subgroup of G invariant under ϕ contains g.*

Proof. The last two statements of the lemma follow at once from the definition of a ϕ-group. To prove the first assertion, let s be the least positive integer such that $g_1 = [g]_r^s$ is in H. Since H is invariant under ϕ, every element of G of the form $\phi^t([g_1]_{r,s}^j)$ is in H. Conversely, if $[g]_r^k \in H$, write $k = sj + t$ and use Lemma 2.1 to get

$$[g]_r^k = [g]_r^{sj}\, \phi^{rsj}([g]_r^t) = [g_1]_{r,s}^j \phi^{rsj}([g]_r^t),$$

whence $[g]_r^t \in H$. Since s is the least positive integer with this property, $t = 0$, and it follows that every element of H is of the form $\phi^t([g_1]_{r,s}^j)$. Thus H is a ϕ-group of index rs with generator $[g]_r^s$.

Finally, we shall establish a simple, but extremely important, relation between the order of ϕ and the order of G.

LEMMA 2.3. *Let G be a ϕ-group of index r with respect to a generator g of G; let h be the order of ϕ and let k be the least integer such that $[g]_r^k = 1$. Then $hk > o(G)$. In particular, if ϕ^r is Frobenius, $k = h/r$.*

Proof. Since every element of G must be in the orbit under ϕ of one of the k elements $[g]_r^j$, $j = 1, 2, \dots, k$, since each of these orbits contains at most h elements, and since the last one of them consists of only the identity element of G, the inequality $hk > o(G)$ is immediate.

If ϕ^r is Frobenius, Lemma 2.1 shows that $[g]_r^{h/r} = 1$. The proof of this equality shows also that for any value of $j < h/r$, $[g]_r^j \neq 1$. Thus $k = h/r$.

3. Automorphisms of a class of groups of order $p^m q^n$. In the next three sections we shall show that a regular ϕ-group in which no subgroup has an exceptional group as a composition factor is nilpotent. The heart of

the problem is to prove this result for certain ϕ-groups of order $p^m q^n$; §§ 3 and 4 are devoted to this special case.

LEMMA 3.1. *Let G be a group of order $p^m q^n$, p and q being primes, in which the p-Sylow subgroup P is normal in G and Abelian of type $(p, p, \ldots, p)$, while the q-Sylow subgroups are Abelian of type $(q, q, \ldots, q)$; and assume that the centre of G is trivial. Suppose ϕ is an automorphism of G of order h such that no proper subgroup of P which is invariant under ϕ is normal in G and such that some q-Sylow subgroup Q, but no proper subgroup of Q, is invariant under ϕ. Then if d is the order of ϕ on Q, we have $d|m$ and $h|d(p^{m/d} - 1)$.*

Proof. Since G has no centre, $p \neq q$ and $m, n > 0$.

Since each element y in Q induces by conjugation an automorphism ψ_y of P, there exists a group of automorphisms A acting on P which can be expressed in the form $\bar{Q}R$, where $\bar{Q}$ is normal in A and is isomorphic to Q under the correspondence $\psi_y \leftrightarrow y$, where R is the cyclic subgroup generated by ϕ, and where

$$\phi^{-1}\psi_y\phi = \psi_{\phi(y)} \text{ for all } y \text{ in } Q. \tag{1}$$

For all y in Q, we have $\phi^d(y) = y$, and hence $\phi^{-d}\psi_y\phi^d = \psi_y$. Thus ϕ^d is in the centre of A, and since Q is Abelian, the subgroup A_0 generated by ϕ^d and $\bar{Q}$ is Abelian.

We shall regard P as an m-dimensional vector space over the prime field K with p-elements, and A as a group of linear transformations acting on P. If K^* denotes the algebraic closure of K and P^*, the m-dimensional vector space over K^*, we may also consider A as a group of linear transformations on P^*.

Now let W be a minimal subspace of P, invariant under ϕ, and of dimension t, and let $f(x)$, of degree t and irreducible over K, be the minimal polynomial of ϕ^d on W. Since ϕ^d is in the centre of A, the subspaces $\phi^i\psi_y(W)$ are invariant under ϕ^d for all i and all y in Q, and ϕ^d has the same minimal polynomial $f(x)$ on each of these subspaces. Let

$$P_0 = \sum_{i,y} \phi^i\psi_y(W).$$

It follows immediately from (1) that P_0 is left fixed by every element of A. Regarded as a subgroup of P, P_0 is thus normal in G and invariant under ϕ, whence by our hypotheses $P_0 = P$. Since now P is the sum of minimal subspaces invariant under ϕ^d, it follows that P is the direct sum of subspaces $W_1, W_2, \ldots, W_s$, each of dimension t, each invariant under ϕ^d, and on each of which the minimal polynomial of ϕ^d is $f(x)$. Thus

$$m = st \text{ and } f(x)^s \text{ is the characteristic polynomial of } \phi^d \text{ on } P. \tag{2}$$

The order w of ϕ^d on P is the same as its order on each of the subspaces W_i, and since $f(x)$ is irreducible, it follows that $w|p^t - 1$. In particular, this

implies $(w, p) = 1$, and hence that the order of A_0 is relatively prime to p. It follows that the representation of A_0 in P^* is completely reducible.

Now A_0 is Abelian and P^* has coefficients in an algebraically closed field; hence we can find a vector $x_1 \neq 0$ in P^* which is a common characteristic vector of every element in A_0. We shall show that for $0 \leqslant i < d$ the vectors $\phi^i(x_1)$ are also common characteristic vectors of A_0 and that they generate a d-dimensional subspace of P^*, invariant under A.

For each y in Q, we have

$$\psi_{\phi^i(y)}(x_1) = a_{iy}x_1 \tag{3}$$

for some element a_{iy} in K^*. Thus $\phi^{-i}\psi_y\phi^i(x_1) = \psi_{\phi^i(y)}(x_1) = a_{iy}x_1$, so that $\psi_y(\phi^i(x_1)) = a_{iy}\phi^i(x_1)$, proving that $\phi^i(x_1)$ is a common characteristic vector of the elements of $\bar{Q}$. Since ϕ^{di} and ϕ^i commute, $\phi^i(x_1)$ is also a characteristic vector of ϕ^{di}, and hence of every element of A_0.

Let P^*_1 be the subspace of P^* generated by the vectors $\phi^i(x_1)$. Since $\phi^d(x_1) = b_1x_1$ for some b_1 in K^*, P^*_1 is invariant under A; furthermore, the vectors $x_1, \phi(x_1), \ldots, \phi^d(x_1)$ are linearly dependent and hence dim $P^*_1 \leqslant d$.

Suppose if possible that dim $P^*_1 = k < d$. Then for $0 \leqslant i < k$ the vectors $\phi^i(x_1)$ are linearly independent, and furthermore

$$\phi^k(x_1) = c_0x_1 + c_1\phi(x_1) + \ldots + c_{k-1}\phi^{k-1}(x_1), c_j \in K^*, \tag{4}$$

and $c_0 \neq 0$. Apply ψ_y to (4) and use (3) to obtain

$$a_{ky}\phi^k(x_1) = c_0a_{0y}x_1 + c_1a_{1y}\phi(x_1) + \ldots + c_{k-1}a_{k-1y}\phi^{k-1}(y). \tag{5}$$

Now multiply (4) by a_{ky} and subtract from (5), obtaining

$$c_0(a_{0y} - a_{ky})x_1 + c_1(a_{1y} - a_{ky})\phi(x_1) + \ldots + c_{k-1}(a_{k-1y} - a_{ky})\phi^{k-1}(x_1) = 0.$$

Since $x_1, \phi(x_1), \ldots, \phi^{k-1}(x_1)$ are linearly independent and since $c_0 \neq 0$, we conclude that

$$a_{ky} = a_{0y}. \tag{6}$$

But (6) implies

$$\phi^{-k}\psi_y^{-1}\phi^k\psi_y(x_1) = a_{0y}\phi^{-k}\psi_y^{-1}\phi^k(x_1) = a_{0y}a_{ky}^{-1}x_1 = x_1.$$

Thus x_1 is a common characteristic vector of all commutators $\phi^{-k}\psi_y^{-1}\phi^k\psi_y$, $y \in Q$, with the common characteristic root 1. Since these linear transformations are defined over K and 1 is in K, it is easy to show that they have a common characteristic vector $z_1 \neq 0$ in P with a common characteristic root 1. But then

$$\phi^{-k}\psi_y^{-1}\phi^k\psi_y(x_1) = \phi^{-k}(y(\phi^k(y^{-1}z_1y))y^{-1}) = z_1,$$

and it follows that $\phi^{-k}(y)y^{-1}$ is in the centralizer of $\phi^k(z_1)$ for all y in Q. But Q is Abelian and hence the set of elements $\phi^{-k}(y)y^{-1}$ form a subgroup Q_0 of Q, which is clearly invariant under ϕ. Since $k < d$ and d is the order of ϕ

on Q, $Q_0 \neq 1$ and our hypotheses imply that $Q_0 = Q$. Thus $\phi^k(z_1)$ commutes elementwise with Q, and since P is Abelian, lies in the centre of G, contrary to the fact that G has a trivial centre. Thus $\dim P^*_1 = d$, as asserted, and with respect to this basis, ϕ is represented on P^*_1 by the companion matrix

$$\Phi_1 = \begin{pmatrix} 0 & 1 & 0 & . & . & . & 0 \\ 0 & 0 & 1 & . & . & . & 0 \\ & & & & & & \\ 0 & 0 & 0 & . & . & . & 1 \\ b_1 & 0 & 0 & . & . & . & 0 \end{pmatrix}. \tag{7}$$

Since A_0 is completely reducible and leaves P^* invariant, we can write $P^* = P_1 \oplus P'$, where P' is invariant under A_0. If $P' \neq 0$, we can construct as above a d-dimensional subspace $P^*_2 \subset P'$, invariant under A, and with respect to a suitable basis of P^*_2, ϕ will be represented by a companion matrix Φ_2, of the same form as Φ_1, with possibly a different element b_2 in the dth row, 1st column. Continuing this process, we can represent P^* as the direct sum of subspaces $P^*_1, P^*_2, \ldots, P^*_\lambda$, each invariant under A and of dimension d, and with respect to a suitable basis of P^*, ϕ is represented by the matrix

$$\phi = \begin{pmatrix} \Phi_1 & & & & \\ & \Phi_2 & & & \\ & & . & & \\ & & & . & \\ & & & & \Phi_\lambda \end{pmatrix} \tag{8}$$

where each Φ_i is a companion matrix of the form (7), having some element b_i of K^* in its dth row, 1st column. In particular,

$$m = d\lambda. \tag{9}$$

From (8) we see that the characteristic polynomial of ϕ over P^* is $g(x) = (x^d - b_1)(x^d - b_2) \ldots (x^d - b_\lambda)$ and that the characteristic polynomial of ϕ^d is $h(x)^d = [(x - b_1)(x - b_2) \ldots (x - b_\lambda)]^d$. Since ϕ is defined over P, the coefficients of $g(x)$ and hence of $h(x)$ are in K. A comparison with (2) now yields

$$f(x)^s = h(x)^d. \tag{10}$$

But $f(x)$ is irreducible, and hence $d|s$ and $h(x) = f(x)^{s/d}$. It follows that the roots $b_1, \ldots, b_\lambda$ of $h(x)$ are roots of $f(x)$ and hence lie in the field with p^t elements. Since $ts = m$ and $d|s$ the quantities b_i lie in the field with $p^{m/d}$ elements, and hence have orders dividing $p^{m/d} - 1$. But by (8) ϕ^d is a diagonal matrix with $b_1, b_2, \ldots, b_\lambda$ as diagonal entries, and it follows that the order of ϕ^d divides $p^{m/d} - 1$, which completes the proof of the lemma.

LEMMA 3.2. *If G satsifies the hypotheses of the preceding lemma, let F denote*

the set of elements of G left fixed by ϕ^r, for some fixed integer r. Then either $F \subset P$, $F = Q$, or $F = G$.

Proof. If $F \not\subset P$, there exists an element z in F with $z = xy$, x in P, and $y \neq 1$ in Q. We have $xy = z = \phi^r(z) = \phi^r(x)\phi^r(y)$, whence $x\phi^r(x^{-1}) = y\phi^r(y^{-1})$. Since the left side of this equation is an element of P, while the right is an element of Q, each is the identity, and so $\phi^r(y) = y$. Thus $y \in Q \cap F$, which is invariant under ϕ. But $Q \cap F \neq 1$ and it follows from the hypotheses of Lemma 3.1 that $Q \cap F = Q$. Thus either $F \subset P$ or $Q \subset F$.

Suppose now that $F > Q$, whence $F \cap P \neq 1$. If $x \in F \cap P$, $\phi^r(yxy^{-1}) = \phi^r(y)\phi^r(x)\phi^r(y^{-1}) = yxy^{-1}$, and hence yxy^{-1} is in $F \cap P$ for any y in Q. Thus $F \cap P$ is normal in G, and being invariant under ϕ, must equal P. Thus F contains P as well as Q, and we conclude that $F = G$.

4. ϕ-groups of order p^mq^n. We shall need a preliminary lemma.

LEMMA 4.1. *Let G be an Abelian ϕ-group of index r, of order p^m and of type $(p, p, \ldots, p)$ and let h be the order of ϕ. Suppose $d|r$, $d|m$, and $h|d(p^{m/d} - 1)$. Then either $d = 1$ or $d = 2$, $r \neq 0$, and the subgroup F left elementwise fixed by ϕ^r has order p.*

Proof. Let $s = m/d$. Since $o(\phi^d)|p^s - 1$, ϕ^d is completely reducible when considered as a linear transformation, and each of its irreducible constituents has dimension $\leqslant s$. Thus G is the direct product of subgroups $G_1, G_2, \ldots, G_k$ invariant under ϕ^d, each of order $\leqslant p^s$ and $k \geqslant d$.

Let g be a generator of G under ϕ of index r and write $g = g_1g_2 \cdots g_k$, $g_i \in G_i$, $i = 1, 2, \ldots, k$. Since G is Abelian, we have

$$[g]_r^j = \prod_{i=1}^{d} [g_i]_r^j. \tag{11}$$

Since ϕ^d leaves G_i invariant and since $d|r$, it follows that $[g_i]_r^j \in G_i$ for all i, j.

Suppose first that $r = 0$. Then $[g]_r^p = 1$ and we have $hp > o(G)$, whence $d(p^s - 1) > p^{sd-1}$, which implies $d = 1$ or $d = 2$, $s = 1$, and $h = 2(p - 1)$.

On the other hand, if $r \neq 0$, the element

$$[g_i]_r^{p^s-1}$$

has order 1 or p and is invariant under ϕ^r, whence by (11) the same is true of

$$[g]_r^{p^s-1}.$$

It follows in either case that

$$[g]_r^{p(p^s-1)} = 1$$

and hence that $h(p(p^s - 1)) > o(G)$. Thus

$$d(p^s - 1)^2 > p^{sd-1}. \tag{12}$$

The only solutions of (12) are $d = 1$, $d = 2$, or $d = 3$, $s = 1$, and $h = 3(p-1)$.

In the third case the G_i are cyclic of order p, for $i = 1, 2, 3$ and are permuted cyclically by ϕ. But then if the subgroup F left elementwise fixed by ϕ^r were to contain some G_i, it would follow that $F = G$, whence G would be of index 0 which is not the case. It follows that $F = 1$ and hence that $[g]_r^{p-1} = 1$. This leads, as in (12), to the inequality $3(p-1)^2 > p^2$, which is impossible.

We show next that $d = 2$, $h = 2(p^s - 1)$ is impossible. In this case $G = G_1 \otimes G_2$ where G_1, G_2 are invariant under ϕ^2, of order p^s, and are permuted by ϕ. If either $g_1 = 1$ or $g_2 = 1$ $\phi^i([g]_r^j) \in G_1 \cup G_2$, which is a proper subset of G. Thus we must have $g = g_1g_2$ with $g_1 \neq 1$, $g_2 \neq 1$. But now ϕ^2 has order $p^s - 1$ on both G_1 and G_2 and so $[g_2]_r^j = 1$ implies $[g_1]_r^j = 1$. Thus the identity is the only element of G_1 which is of the form $\phi^i([g]_r^j)$, contrary to the fact that G is a ϕ-group.

Suppose next that $d = 2$ and $h < 2(p^s - 1)$. Since $h|2(p^s - 1)$, we conclude that $h < p^s - 1$. But now $[g]_r^{h/r} = 1$ implies $h^2/r > p^{2s}$ which is clearly impossible. Thus $[g]_r^{h/r} = x \neq 1$. Since $\phi^r(x) = x$, the subgroup F left elementwise fixed by ϕ^r is not the identity. On the other hand, $[g]_r^{ph/r} = 1$ and so $h(h/r)p > p^{2s}$. It follows that $r < p$. Now F is of index 0, and hence every element of F is of the form $\phi^i(y^j)$ for some element y in F. But ϕ has order r on F, and consequently $rp > o(F)$. Since $r < p$, we conclude that F is cyclic, and the lemma is proved.

We are now ready to prove our main result concerning ϕ-groups of order p^mq^n.

LEMMA 4.2. *If a ϕ-group satisfies the conditions of Lemma* 3.1, *then ϕ leaves some element other than the identity fixed.*

Proof. Let g be a generator of G under ϕ of index r, and let F be the subgroup of G of fixed elements under ϕ^r. According to Lemma 3.2 either $F \subset P$, $F = Q$, or $F = G$.

Case 1. $F \subset P$. Write $g = xy$, with x in P, y in Q. P is normal in G, and hence $[g]_r^j = x_j[y]_r^j$ for some x_j in P. If t is the least integer such that $[y]_r^t = 1$, then t is the least integer such that $[g]_r^t$ is in P, and hence P is a ϕ-group of index rt. Moreover, since Q is Abelian, it follows that $\phi^{rt}(y) = y$. But now the subgroup of Q left fixed elementwise by ϕ^{rt} is invariant under ϕ and contains y, whence by our hypotheses it must equal Q. Thus the order d of ϕ on Q divides rt, the index of P. In view of Lemma 3.1, P now satisfies all the conditions of Lemma 4.1, and hence either $d = 1$, in which case ϕ is the identity on Q, or $d = 2$ and the subgroup F_1 of P left elementwise fixed by ϕ^{rt} is cyclic.

In the latter case, ϕ^r leaves only the identity element of Q fixed, since $F \subset P$, and hence ϕ^r has order 2 on Q. It follows that $\phi^r(z) = z^{-1}$ for all z in Q. In particular this implies $t = 2$. Furthermore if ψ_z denotes the automorphism of P induced by conjugation by an element z in Q, we also have

$\phi^{2r}\psi_z\phi^{-2r} = \psi_z$. If $F_1 = (x_1)$, we conclude at once that $\phi^{2r}(\psi_z(x_1)) = \psi_z(x_1)$, whence $\psi_z(x_1) \in F_1$ for all z in F_1. Thus F_1 is normal in G, and being invariant under ϕ, $F_1 = P$, whence $o(P) = p$. Hence $m = 1$, contrary to the fact that $d|m$ by Lemma 3.1.

Case 2. $F = Q$. Since $F \neq G$, $r \neq 0$. If $r = 1$, every element of Q is left fixed by ϕ. Hence we may assume $r > 1$. We have $[y]_r^q = y^q = 1$, and hence $x_q = [g]_r^q \in P$. Since ϕ^r is without non-trivial fixed elements on P, $[x_q]_r^{h/r} = 1$, $[g]_r^{qh/r} = 1$, and $h^2q > ro(G)$ by Lemma 2.3. Since $h|d(p^{m/d} - 1)$, we have

$$d^2(p^{m/d} - 1)^2 > rp^mq^{n-1}. \tag{13}$$

The only solutions of (13) are $d = 1$, in which case the lemma follows, or $d = 2$ and $r = 2, 3$. If $d = 2$, ϕ^2 leaves Q elementwise fixed, while if $r = 3$, ϕ^3 leaves Q elementwise fixed. Hence the case $d = 2$, $r = 3$ implies ϕ is the identity on Q. In the remaining case $d = 2$, $r = 2$, we have $d|r$ and hence by Lemma 4.1, the subgroup F_1 of P left elementwise fixed by ϕ^{2q} is cyclic (since P is of index $2q$). This leads to a contradiction as in Case 1.

Case 3. $F = G$. This is the case $r = 0$. P is also of index 0, so that d divides the index of P, whence by Lemma 4.1, $d = 1$. Thus ϕ is the identity on Q, and the lemma is established.

We wish to point out that there do exist ϕ-groups satisfying the conditions of Lemma 3.1 in which ϕ leaves some non-trivial element of G fixed. Perhaps the simplest example is the symmetric group S_3 on three letters, which can be defined by the relations $x^3 = y^2 = 1$ and $y\,xy^{-1} = x^{-1}$. It is easily checked that S_3 is a ϕ-group of index 1 with respect to the automorphism ϕ defined by: $\phi(x^iy^j) = x^{-i}y^j$, the element xy being a generator of S_3 under ϕ.

5. Solvable and non-exceptional ϕ-groups. A group G is called *exceptional* if G is a non-cyclic simple group in which the normalizer of every characteristic subgroup $\neq 1$ of a p-Sylow subgroup P of G is P, for all primes $p|o(G)$. It is easily shown that if G is solvable or if every Sylow subgroup of G is Abelian, then no subgroup of G has a composition factor which is an exceptional group (**2**, Lemma 4.1).

THEOREM 1. *Let G be a regular ϕ-group and assume that no subgroup of G has a composition factor which is an exceptional group. Then G is nilpotent.*

Proof. The proof is by induction on the order of G, and consists in reducing to the case in which G satisfies the conditions of Lemma 3.1. This reduction is almost identical with that given by Feit (**2**, Lemma 4.2 and Theorem). However, as our group G need not be the regular subgroup of a Frobenius group, we shall outline the steps in this portion of the proof.

We first show that G contains a normal subgroup of prime power order invariant under ϕ. If G has a proper characteristic subgroup H, H is nilpotent by induction, and any of its Sylow subgroups are normal in G and invariant

under ϕ. Otherwise G is the direct product of isomorphic non-exceptional simple groups. There exists then some $p|o(G)$ such that a p-Sylow subgroup P of G contains a characteristic subgroup T such that $N(T) > P$. Since ϕ is a Frobenius automorphism, some p-Sylow subgroup of G is invariant under ϕ, and we may assume it to be P. Either T is normal in G (and $\phi(T) = T$) or by induction $N(T)$ is nilpotent, P is normal in $N(T)$, and hence $N(P) > P$. Either the centre C of P is normal in G, and invariant under ϕ or $N(C)$ is nilpotent.

If neither C nor T is normal in G, we have $N(C) \supset N(P) > P$. If Q is the unique q-Sylow subgroup of $N(C)$ for some prime $q \neq p$, and if Q is not normal in G, $N(Q)$ is nilpotent and contains P, whence P and Q commute elementwise. If $C \supset x\,Px^{-1}$, then $Q \supset N(x^{-1}Cx)$, which is nilpotent, so that Q commutes elementwise with $x^{-1}Px$ as well as P. Since $N(Q)$ is nilpotent, $x^{-1}Px = P$, and it follows that G is p-normal. But $N(P)$ is also nilpotent, so that by a theorem of Grün (**6**, p. 171) G contains a normal subgroup H such that $G/H \cong C$, contradicting the fact that G is its own commutator subgroup. Thus G contains a normal subgroup of prime power order, invariant under ϕ.

Let P be a minimal such subgroup so that P is Abelian of type $(p, p, \ldots, p)$. By induction G/P is nilpotent. If G is not a p-group, suppose q is a prime dividing $o(G)$, $q \neq p$; and let Q be a minimal subgroup invariant under ϕ of a q-Sylow subgroup of G. If $PQ < G$, PQ is nilpotent and this, together with the fact that G/P is nilpotent, implies that Q is in the centre of G. But then G/Q and hence G is nilpotent.

We may suppose therefore that $G = PQ$, the centre of G is trivial, no subgroup of P invariant under ϕ is normal in G, and no subgroup of Q is invariant under ϕ—precisely the hypotheses of Lemma 3.1. But now Lemma 4.2 implies that there is no regular ϕ-group which satisfies these conditions, and hence G is nilpotent.

COROLLARY. *If the Sylow subgroups of a regular ϕ-group are G Abelian, then G is Abelian.*

6. The fixed subgroup of ϕ^r. The subgroup left elementwise fixed by ϕ^r plays an important role in determining the structure of a ϕ-group of index r. In this section we shall determine some of the properties of this subgroup for ϕ-groups of prime power order. We shall need the following lemma:

LEMMA 6.1. *Let G be a ϕ-group of index 0 of order p^n having a generator g of order p^n. Then G contains a sequence of characteristic subgroups $G = G_n \supset G_{n-1} \supset \ldots \supset G_1 \supset G_0 = 1$ where G_i is generated by the elements of order p^i in G. Moreover, the subgroups G_i are the only subgroups of G invariant under ϕ.*

Proof. Since G is a ϕ-group of index 0, the elements $\phi^t(g^{p^{n-1}})$ clearly include all elements of order p in G. Since no proper subset of these elements form a

subgroup invariant under ϕ, they must form the characteristic subgroup G_1 of elements of order dividing p in the centre of G. As pointed out, no proper subgroup of G_1 is invariant under ϕ.

The lemma follows now easily by applying induction to the group G/G_1.

THEOREM 2. *Let G be a regular ϕ-group of index r and order p^a, and let F be the subgroup of G left elementwise fixed by ϕ^r. Then every subgroup of F invariant under ϕ is normal in G.*

Proof. Since ϕ^r leaves F elementwise fixed, F is of index 0, and hence by the preceding lemma the elements of order p in F form a characteristic subgroup F_1 of F. If F_1 is normal in G, the theorem follows by induction. For if we set $\bar{G} = G/F_1$, $\bar{F}$ = the residue of F in $\bar{G}$, and $\bar{F}'$ the subgroup of elements left elementwise fixed by the image $\bar{\phi}^r$ of ϕ^r, $\bar{F} \subset \bar{F}'$ and $\bar{F}'$ is normal in $\bar{G}$ by induction. Since $\bar{F}$ is invariant under $\bar{\phi}$, $\bar{F}$ is characteristic in $\bar{F}'$ by the preceding lemma, and hence normal in $\bar{G}$. Thus F is normal in G and the theorem follows at once.

We shall actually prove that F_1 lies in the centre of G. Let h be the order of ϕ, let g be a generator of G under ϕ, and let

$$g_1 = [g]_r^{h_1/r}$$

be a generator of F_1, so that F_1 is of index h_1. To our induction hypothesis we shall add the assertion that either h/h_1 or h_1/h is a power of p.

Let us begin by verifying this statement under the assumption that F_1 is in the centre of G. Let k be the order of $\bar{\phi}$ of $\bar{G}$ and let $\bar{g}$ be the residue of g in $\bar{G}$. Let H be the set of elements of G left fixed by ϕ^k and suppose first the $H \not\supset F_1$. Then $H \cap F_1 = 1$ and hence ϕ^k is Frobenius on F_1. Thus $\phi^k(g) = xg$, $x \in F_1$ and $x = y^{-1}\phi^k(y)$ for some y in F_1. It follows that $\phi^k(gy^{-1}) = gy^{-1}$, whence $gy^{-1} \in H$. Thus $g \in F_1H$. Since F_1H is invariant under ϕ and contains g, $G = F_1H$. Since $H \cong \bar{G}$, ϕ has order k on H. If $(r, k) = s$, it follows that

$$h = \frac{rk}{s}. \tag{14}$$

On the other hand, let H_1 be the subgroup of H generated by the elements of order p left elementwise fixed by ϕ^r. Then F_1H_1 is left elementwise fixed by ϕ^r and its elements all have order dividing p. It follows that $F_1H_1 = F_1$. Since $F_1 \cap H_1 = 1$, we conclude that $H_1 = 1$. Hence ϕ^r leaves only the identity element of H fixed, and consequently $\bar{\phi}^r$ leaves only the identity element of $\bar{G}$ fixed. But this implies k/s is the least integer such that $[\bar{g}]_r^{k/s} = 1$, and hence $g_1 = [g]_r^{k/s}$. Thus rk/s is the index of F_1, and in view of (14) we conclude that $h_1 = h$.

Hence we may suppose $H \supset F_1$. In this case, the relation $\phi^k(g) = xg$ implies $\phi^{kp}(g) = g$, and we have

$$k|h|kp. \tag{15}$$

Since $r|h$, it follows that either $r = s$ or $r = sp$. If $\bar{\phi}^r$ leaves only the identity element of $\bar{G}$ fixed, it follows as above that $h_1 = kr/s$, and hence $k|h_1|kp$. We conclude from (15) that either h/h_1 or h_1/h is a power of p.

If $\bar{\phi}^r$ is not Frobenius, let $\bar{F}_1$ be the subgroup of $\bar{G}$ generated by the elements of order p left elementwise fixed by $\bar{\phi}^r$. If k_1 is the index of $\bar{F}_1$, then by induction either k/k_1 or k_1/k is a power of p. By definition of k_1,

$$[\bar{g}]_r^{k_1/r}$$

is a generator of $\bar{F}_1$, and hence

$$g_2 = [g]_r^{k_1/r}$$

is a generator of the inverse image F_2 of $\bar{F}_1$. Since $\bar{\phi}^r$ leave $\bar{F}_1$ elementwise fixed and $r|k_1$,

$$\phi^{k_1}(g_2) = zg_2$$

for some z in F_1. Since F_1 is in the centre of F_2, this implies

$$[g_2]_{k_1}^j = z^{j(j-1)/2} g_2^j. \tag{16}$$

As p is the least power of j for which $g_2^j \in F_1$, it follows at once that $h_1 = k_1 p$. Thus $h_1 = kp^\epsilon$ for some integer ϵ. This together with (15) implies that either h/h_1 or h_1/h is a power of p.

Finally we must show that F_1 does in fact lie in the centre of G. Let C be a minimal subgroup of the centre of G invariant under ϕ. Because of the minimality of F_1, either $C = F_1$ or $C \cap F_1 = 1$. In the latter case, let $\bar{G}$, $\bar{F}_1$, $\bar{g}$, $\bar{\phi}$ be respectively G/C, the image of F_1 and g in G/C, and the image of ϕ on G/C. Let m be the order of $\bar{G}$ on $\bar{F}$, and define M to be the subgroup of G left elementwise fixed by ϕ^m.

Now by induction, if m_1 is the index of $\bar{F}_1$, we have

$$\frac{m}{m_1} = p^\epsilon \tag{17}$$

for some integer ϵ.

By definition of m_1, $r|m_1$. If we write $r = r_1 p^\delta$, where $(r_1, p) = 1$, it follows that

$$r_1|m. \tag{18}$$

Since every element of F_1 is of the form $\phi^i(g_1^j)$, the order of ϕ on F_1 is relatively prime to p, and hence ϕ^{r_1} leaves F_1 elementwise fixed. It follows therefore from (18) that $F_1 \subset M$.

Assume first that $C \subset M$, in which case $CF_1 \subset M$. Now the index of CF_1 = index of $\bar{F}_1 = m_1$. Let g' be a generator of CF_1 of index m_1 and write $g' = xy$, $x \in C$, $y \in F_1$. If $m|m_1$,

$$[g']_m^j = g'^j = x^j y^j,$$

and every element of CF_1 is of the form $\phi^i(x^iy^j)$, which is clearly impossible since $C \cap F_1 = 1$. On the other hand, if $m \not\equiv m_1$ (17) holds with $\epsilon \supset 0$, and in this case

$$[g^r]^j_{m_1} = [x]^j_{m_1} y^j. \tag{19}$$

To obtain an element of F_1, we must have

$$[x]^j_{m_1} = 1,$$

and this implies $\phi^{m_1 j}(x) = x$ since C is Abelian. If $j = 1$,

$$[g^r]^j_{m_1} = x^j y^j,$$

which is impossible as above. Since

$$\phi^{m_1 p^e}(x) = x,$$

$j \not\equiv 1$ implies $p|j$ and hence 1 is the only element of F_1 which can be written in the form

$$\phi^i([g^r]^j_{m_1}),$$

contrary to the fact that g^r is a generator of CF_1 under ϕ.

On the other hand, if $C \cap M = 1$, it follows as in an earlier part of the proof that $G = CM$. But $M < G$ and $F_1 \subset M$ so that by induction F_1 is in the centre of M. Since C is in the centre of G, it follows that F_1 is in the centre of G, and the proof is complete.

COROLLARY. *If F_1 denotes the subgroup of F generated by the elements of order p in F, then F_1 lies in the centre of G.*

7. ϕ-groups in which ϕ^r leaves only the identity fixed. We shall also need some properties of ϕ-groups of index r in which ϕ^r is a Frobenius automorphism. To this end, we first establish the following lemma.

LEMMA 7.1. *Let G be a regular ϕ-group of prime power order, and let C be a subgroup of the centre of G, invariant under ϕ and of least possible order. Then either $C = G$ or $[o(C)]^2 \leqslant o(G)$.*

Proof. We may suppose $G > C$. If $\bar{G} = G/C$, we may restrict our attention to a minimal subgroup of the centre of $\bar{G}$, and hence without loss of generality we may assume that $\bar{G}$ is Abelian of type $(p, p, \ldots, p)$ and that no proper subgroup of $\bar{G}$ is invariant under the image $\bar{\phi}$ of ϕ on $\bar{G}$.

Let g be a generator of G, $\bar{g}$ its image in $\bar{G}$, k the order of $\bar{\phi}$, and H the subgroup of G left elementwise fixed by ϕ^k. If $H \cap C = 1$, it follows as in the preceding section that $G = CH$. Since $G/C \cong H$, H, and hence G, is Abelian. But by definition of C, $o(C) \leqslant o(H)$ and therefore $[o(C)]^2 \leqslant o(G)$.

If, on the other hand, $H \supset C$, the equation $\phi^k(g) = yg$ implies $\phi^{kp}(g) = g$ so that $h|kp$, where h is the order of ϕ. If $h = k$ and ϕ^r leaves only the identity element fixed, it follows as in the preceding section that the identity is the

only element C which can be written in the form $\phi^t([g]_r^s)$, which is a contradiction.

If $h = k$ and some proper subgroup F of G is left elementwise fixed by ϕ^k, either $F \cap C = 1$ or $F \supset C$. In the first case, since no proper subgroup of $\bar{G}$ is invariant under $\bar{\phi}$, it follows that $G = CF$, and hence G is Abelian since $F \cong \bar{G}$ is Abelian; and we have $[o(C)]^2 \leqslant o(G)$.

If $F > C$, then $F = G$ is of index 0, and hence C contains all elements of G of order p. If $\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_m$ are a basis of $\bar{G}$, let $x_1, x_2, \ldots, x_m$ be a set of representatives such that $\phi(x_i) = x_{i+1}$, $i = 1, 2, \ldots, m-1$. Then

$$\phi(x_m) = z x_1^{a_1} x_2^{a_2} \ldots x_m^{a_m}.$$

Since $x_i^p \in C$ for all i, it follows at once that $x_1^p, x_2^p, \ldots, x_m^p$ generate a subgroup C_1 of C invariant under ϕ. Since C is minimal, $C_1 = C$, and hence $o(C) \leqslant p^m = o(\bar{G})$, which implies $[o(C)]^2 \leqslant o(G)$.

Finally if $F = C$, C is of index 0, whence the order of ϕ on G is a multiple of $\frac{p^n - 1}{p - 1}$, where $p^n = o(C)$. This implies $(p^n - 1)/(p - 1) | k$. But $\bar{G}$ is an Abelian group of type $(p, p, \ldots, p)$ and hence $k < o(\bar{G})$. Thus $o(C) = p^n \leqslant o(\bar{G})$ and $[o(C)]^2 \leqslant o(G)$, as desired.

We now prove

THEOREM 3. *Let G be a regular ϕ-group of index r and assume ϕ^r leaves only the identity element of G fixed. Then either some Sylow subgroup of G is Abelian or there exists a proper subgroup G_1 in G, invariant under ϕ, which contains a non-trivial subgroup of the centre of some p-Sylow subgroup of G for every prime $p | o(G)$.*

Proof. If g is a generator of G under ϕ, and if h denotes as usual the order of ϕ, we have first of all $[g]_r^{h/r} = 1$ and hence by Lemma 2.3

$$h^2 > o(G). \tag{20}$$

Let $p_1, \ldots, p_t$ be the distinct primes dividing $o(G)$, and let $P_1, \ldots, P_t$ be the corresponding Sylow subgroups of G invariant under ϕ. Let C_i be a minimal subgroup of P_i, invariant under ϕ, and of lowest possible order. Then if no Sylow subgroup of G is Abelian, the preceding lemma gives

$$[o(C_i)]^2 \leqslant o(P_i), \qquad i = 1, 2, \ldots, t. \tag{21}$$

Define s_i by the condition that

$$g_i = [g]_r^{s_i}$$

be a generator of Ci, and let h_i be the order of ϕ on C_i, $i = 1, 2, \ldots, t$. Since C_i is an Abelian group of type $(p_i, p_i, \ldots, p_i)$, we have

$$h_i < o(C_i), \qquad i = 1, 2, \ldots, t. \tag{22}$$

Now let λ be the greatest common divisor of $s_1, s_2, \ldots, s_t$. We may assume the s_i are so numbered that

$$\lambda = \sum_{i=1}^{m} a_i s_i - \sum_{i=m+1}^{t} b_i s_i, \qquad \text{where } a_i, b_i \geqslant 0. \tag{23}$$

We now consider the elements

$$\begin{aligned} x &= [g_1]_{rs_1}^{a_1} \phi^{rs_1 s_1}([g_2]_{rs_2}^{a_2}) \cdots \phi^{r(a_1 s_1 + \ldots + a_{m-1} s_{m-1})}([g_m]_{rs_m}^{a_m}) \\ y &= [g_{m+1}]_{rs_{m+1}}^{b_{m+1}} \phi^{rb_{m+1} s_{m+1}}([g_{m+2}]_{rs_{m+2}}^{b_{m+2}}) \cdots \phi^{r(b_{m+1} s_{m+1} + \ldots + b_{t-1} s_{t-1})}([g_t]_{rs_t}^{b_t}). \end{aligned} \tag{24}$$

By repeated use of Lemma 2.1, we find that

$$x = [g]_r^u \quad \text{and} \quad y = [g]_r^v, \qquad \text{where } u = \sum_{i=1}^{m} a_i s_i, v = \sum_{i=m+1}^{t} b_i s_i, \tag{25}$$

and hence that $z = y^{-1}x = \phi^{rv}(g)\phi^{r(v+1)}(g) \cdots \phi^{r(u-1)}(g)$. It follows that

$$z = \phi^{rv}([g]_r^\lambda). \tag{26}$$

By construction z is a power product of elements of $C_1, C_2, \ldots, C_t$, and hence we have $\phi^k(z) = z$ for some integer $k \mid \Pi_1^t h_i$. Therefore

$$\phi^k([g]_r^\lambda) = [g]_r^\lambda \quad \text{with} \quad k \,\Big|\, \prod_{i=1}^{t} h_i. \tag{27}$$

Now let G_1 be the subgroup of G invariant under ϕ which is generated by $[g]_r^\lambda$. We prove that G_1 is a proper subgroup of G. Suppose, on the contrary, that $G_1 = G$. Then ϕ^k is the identity on G by (27) and hence $h \mid k$.

But then combining (21), (22), and (23), we get

$$h^2 < \prod_{i=1}^{t} h_i^2 < \prod_{i=1}^{t} [o(C_i)]^2 < \prod_{i=1}^{t} (o(P_i)) = o(G), \tag{28}$$

in contradiction to (20).

Since $\lambda \mid s_i$ for all i, $[g]_r^{s_i}$ and hence C_i is contained in G_1 for all $i = 1, 2, \ldots, t$, and the theorem is proved.

COROLLARY. *The same conclusion holds if we assume that $h^2/r > o(G)$ instead of that ϕ^r leaves only the identity element of G fixed.*

8. The structure of regular ϕ-groups. We are now in a position to prove our main result

THEOREM 4. *Every regular ϕ-group is nilpotent.*

Proof. Let G be a regular ϕ-group of index r, g a generator of G under ϕ, and let k be the least integer such that $[g]_r^k = 1$. The proof will be by induction on k.

If H is a proper subgroup of G invariant under ϕ, and s the least integer such that $z = [g]_r^s \in H$, then clearly $s \mid k$, z is a generator of H of index rs and $[z]_{rs}^{k/s} = 1$. Hence by induction H is nilpotent.

It suffices therefore, in view of Theorem 1, to prove that the normalizer

of a characteristic subgroup of some Sylow subgroup P of G contains P properly. As in Theorem 1, we may suppose G contains no proper characteristic subgroup; and hence that G is the direct product of isomorphic non-cycle simple groups, no subset of which is invariant under ϕ.

Let $p_1, p_2, \ldots, p_t$ be the distinct primes dividing $o(G)$, and let $P_1, P_2, \ldots, P_t$ be the corresponding Sylow subgroups of G invariant under ϕ. If, first of all, some P_i is Abelian, $N(P_i) \prec G$, and hence is nilpotent. Thus P_i is in the centre of its normalizer, and it follows by a theorem of Burnside that G contains a normal subgroup H such that $G/H \cong P_i$, contrary to the fact that G is its own commutator subgroup.

Thus no Sylow subgroup of G is Abelian. If ϕ^r left only the identity element of G fixed, it would follow from Theorem 3 that there exists a proper subgroup G_1 in G, invariant under ϕ which contains for each $i = 1, 2, \ldots, t$ a subgroup C_i' of the centre of P_i. Since G_1 is nilpotent by induction and G is not a p-group, $N(C_i') \succ P_i$. Now $N(C_i') \prec G$ and so is nilpotent. If C_i denotes the centre of P_i, it follows that $N(C_i) \succ P_i$, $i = 1, 2, \ldots, t$, and by a previous remark this is sufficient to prove the nilpotency of G. Hence if F denotes the subgroup of G, left elementwise fixed by ϕ^r, $F \succ 1$.

Let $g_i = [g]_r^{s_i}$ be a generator of P_i, $i = 1, 2, \ldots, t$ and define F_i to be the subgroup of G left elementwise fixed by ϕ^{rs_i}. Clearly $F \subset F_i$ for all i. Suppose first there is an index i, say $i = 1$, for which $o(F_1)$ is divisible by at least two distinct primes.

If $F_1 \prec G$, then F_1 is nilpotent by induction. Let P_i' be the p_i-Sylow subgroup of F invariant under ϕ. As is easily seen, $P_i' \subset P_i$. Suppose for some i $p_i | o(F)$. By Theorem 2, $F_i \cap P_i$ is normal in P_i and $F \cap P_i$ being invariant under ϕ, is a characteristic subgroup of $F_i \cap P_i$, and hence is normal in $F_i \cap P_i$ Thus $N(F \cap P_i) \supset P_i$ Since F_1 is nilpotent, it follows that $F \cap P_i$ is normal in F_1, and hence $N(F \cap P_i) \supset F_1$. It follows from our assumption on $o(F_1)$ that $N(F \cap P_i) \succ P_i$. Since $N(F \cap P_i)$ is nilpotent by induction, we conclude that $N(C_i) \succ P_i$ which is sufficient to prove the nilpotency of G.

Suppose instead that $F_1 = G$, so that ϕ^{rs_1} is the identity on G. If g_1 has order p^n, it follows that

$$[g_1]_{rs_1}^{p^n} = g_1^{p^n} = 1, \text{ whence } [g]_r^{s_1 p^n} = 1,$$

and consequently

$$k = s_1 p^n. \tag{29}$$

Since G is not solvable, the well-known theorem of Burnside implies $t \geq 3$. It follows from (29) that $s_2 | s_1 p^n$ and $s_2 | s_1 p^n$. However $s_2 \nmid s_1$, for this would imply that $[g]_r^{s_1} \in P_1 \cap P_2 = 1$, which is not the case. Similarly $s_3 \nmid s_1$, and hence

$$p_1 | s_2, \qquad p_1 | s_3. \tag{30}$$

Let G_1 be the subgroup generated under ϕ by

$$g' = [g]_r^{p^n}.$$

By (30), $G_1 \supset P_2$ and $G_1 \supset P_3$. If $G_1 < G$, G_1 is nilpotent by induction, and consequently $N(C_2) > P_2$, from which the nilpotency of G follows. On the other hand, if $G_1 = G$, g' is a generator of G under ϕ of index rp_1 and

$$[g']_{rp_1}^{k'} = 1, \text{ where } k' = k/p_1.$$

Since $k' < k$, the nilpotency of G follows by induction.

Finally we must consider the case in which each F_i is of prime power. Since $F \subset F_i$ for all i, $o(F_i)$ is a power of a single prime, say p_1, for all $i = 1, 2, \ldots, t$. In particular, this implies $F_i \cap P_i = 1$, $i = 2, 3, \ldots, t$, and ϕ^{rs_i} leaves only the identity element of P_i fixed. Once again $t \geqslant 3$.

It follows at once from the fact that $[g]_r^k = 1$ that $\phi^{rk}(g) = g$, and hence that $(h/r) | k$. Thus

$$k = mh/r \tag{31}$$

for some integer m.

If $m = 1$, $h(h/r) > o(G)$, and it follows from the corollary of Theorem 3 that either some Sylow subgroup of G is Abelian or G contains a proper subgroup G_1 satisfying the conditions of Theorem 3. Since both of these cases have been treated above, we may assume $m > 1$.

On the other hand, since ϕ^{rs_i} leaves only the identity element of P_i fixed,

$$[g_i]_{rs_i}^{h/r} = 1, \qquad i = 2, 3;$$

and hence

$$[g]_r^{hs_i/r} = 1.$$

It follows that

$$m | s_i, \qquad i = 2, 3. \tag{32}$$

If now G^*_1 is the subgroup of G generated under ϕ by $g^* = [g]_r^m$, $G^*_1 \supset P_2$ and $G^*_1 \supset P_3$ in view of (32). If $G^*_1 < G$, it follows as above that $N(C_2) > P_2$ and that G is nilpotent; while if $G^*_1 = G$, g^* is a generator of G of index rm,

$$[g^*]_{rm}^{k^*} = 1,$$

where $k^* = k/m$, and G is nilpotent by induction.

9. The solvability of ϕ-groups. We now prove

THEOREM 5. *Every ϕ-group is solvable.*

Proof. Let G be a ϕ-group of index r with respect to a generator g, and let h be the order of ϕ. As in § 2, we imbed G as a normal subgroup of a group G^* which satisfies the following conditions:

$$G^* = GA \text{ with } G \cap A = 1, \; aya^{-1} = \phi(y) \tag{33}$$

for some element a in G^* of order h and all y in G.

If

$$y = \phi^i([g]_r^j)$$

is an arbitrary element of G, we can represent y in G^* in the form

$$y = a^t[g(a^r g a^{-r})(a^{2r} g a^{-2r}) \dots (a^{(j-1)r} g a^{-(j-1)r}) a^{-t},$$

which reduces to

$$y = a^t (g a^r)^j a^{-jr-t} \tag{34}$$

Setting $b = ga^r$, every element of G can thus be expressed in the form $a^t b^j a^{-jr-t}$ for suitable choice of i and j. If $x \in G^*$, $x = ya^k$ for some y in G and some integer k. It follows that

$$\text{if } x \in G^*,\ x = a^u b^v a^w \text{ for suitable integers } u, v, w. \tag{35}$$

If ϕ leaves only the identity element of G fixed, G is nilpotent by Theorem 4; and so we may assume that there is a subgroup $H \neq 1$ in G which is left elementwise fixed by ϕ.

Let $g_1 = [g]_r{}^s$ be a generator of H, so that by (34)

$$g_1 = b^s a^{-rs}. \tag{36}$$

Since $\phi(g_1) = g_1$, we have $a g_1 a^{-1} = a b^s a^{-rs} a^{-1} = b^s a^{-rs}$, whence

$$a b^s a^{-1} = b^s. \tag{37}$$

Thus b^s commutes with a. Since b^s obviously commutes with b, it follows from (35) that b^s is in the centre of G^*. Let C^* be the subgroup generated by b^s, and set $\bar{G}^* = G^*/C^*$. Denoting the images of a, b, g, G in $\bar{G}^*$ respectively by $\bar{a}$, $\bar{b}$, $\bar{g}$, $\bar{G}$, it follows first of all that $\bar{G}$ is normal in G^*, and secondly that every element of $\bar{G}$ is of the form $\bar{a}^t \bar{b}^j \bar{a}^{-jr-t}$, while every element of $\bar{G}^*$ is of the form $\bar{a}^w \bar{b}^v \bar{a}^w$. If $\bar{\phi}$ denotes the automorphism of $\bar{G}$ induced by conjugation by $\bar{a}$, we can reverse the steps in the derivation of (34) to conclude that every element of $\bar{G}$ is of the form $\bar{\phi}^t([\bar{g}]_r{}^j)$. Thus $\bar{G}$ is a $\bar{\phi}$-group; and by definition of $\bar{\phi}$, we have

$$\bar{\phi}(\bar{y}) = \bar{a}\bar{y}\bar{a}^{-1}, \qquad \bar{y} \in \bar{G}. \tag{38}$$

Either $\bar{\phi}$ leaves only the identity element of $\bar{G}$ fixed or we may repeat the process. Continuing this process we can always construct a sequence of groups

$$G_i^*,\ i = 1, 2, \dots, n \quad \text{with} \quad G^* = G_1^*, \qquad \bar{G}^* = G_2^*,$$

satisfying the following conditions:

(1) $G_{i+1}^* = G_i^*/C_i^*$, where C_i^* is a cyclic subgroup of the centre of G_i^*, $i = 1, 2, \dots, n-1$;

(2) G_n^* is either the identity or contains a normal subgroup G_n such that G/G_n is cyclic;

(3) G_n is a ϕ_n-group in which ϕ_n leaves only the identity element of G_n fixed.

By Theorem 4, G_n is nilpotent. Hence G^*_n and conseqently G^* is solvable. Since $G \subset G^*$, it follows that G is solvable.

Remark. Not every ϕ-group is nilpotent. An example of a non-nilpotent ϕ-group is the symmetric group on 3 letters, which was discussed at the end of § 4.

10. ϕ-groups of index 0. In the next two sections we shall show that a regular ϕ-group of prime power order is either Abelian or metabelian. In view of Theorem 4 this will imply that a regular ϕ-group is nilpotent of class $\leqslant 2$.

In **(4**, Lemma 2**)**, it has been shown that a regular ϕ-group of index 0 is Abelian if the order of ϕ is relatively prime to the order of a generator of G under ϕ. In this section we shall establish the same result without making any restrictions on the order of ϕ.

We have seen in Lemma 6.1 that a ϕ-group G of index 0 and of prime power order contains a sequence of subgroups $G = G_n \supset G_{n-1} \supset \ldots \supset G_1 \supset G_0 = 1$, where the G_i are the only subgroups of G invariant under ϕ, where each G_i is normal in G, and where $x^{-1}\phi^r(x) = 1$ if $x \in G_i$, $i = 0, 1, 2, \ldots, n$. For later purposes we need to investigate ϕ-groups of prime power order which contain such a sequence of subgroups G_i satisfying the first two of these conditions together with following weaker third conditions: if $x \in G_i$, then

$$x^{-1}\phi^r(x) \in G_{i-1}, \qquad i = 0, 1, 2, \ldots, n.$$

We begin with the following lemma.

LEMMA 10.1. *Let G be an Abelian ϕ-group of index r, of order p^{nm} and type $(p^n, p^n, \ldots, p^n)$. Denote by G_i the subgroup generated by the elements of order p^i, and assume that for every x in G_i, $x^{-1}\phi^r(x)$ is in G_{i-1}. Then if h is the order of ϕ, we have $h|p^{n-1}(p^m - 1)$ and either $n = 1$ or $m \leqslant 2$.*

Proof. Let g be a generator of G under ϕ. If $n = 1$, G is of order p^m, of type $(p, p, \ldots, p)$, and $g^{-1}\phi^r(g) = 1$, so that G is of index 0, and every element of G is of the form $\phi^i(g^j)$. Hence the orbit under ϕ of g^j contains exactly h elements, if $0 < j < p$; if the number of distinct such orbits is k, we have $hk + 1 = p^m$, whence $h|p^m - 1$.

If $n > 1$, we proceed by induction to prove the first part of the lemma. G_{n-1} is of type $(p^{n-1}, p^{n-1}, \ldots, p^{n-1})$, of order $p^{(n-1)m}$, and is invariant under ϕ. Since $\phi^r(g) = gy$, $y \in G_{n-1}$ and $\phi^r(y) = yy'$, $y' \in G_{n-2}$, it follows by a direct computation that

$$[g]_r^j = y_j g^{j(j-1)/2} g^j, \qquad \text{where } y_j \in G_{n-2}. \tag{39}$$

From (39) it follows that the least value of j for which $[g]_r^j$ is in G_{n-1} is $j = p$, and that G_{n-1} is of index rp with respect to the generator $[g]_r^p$. Since

$$[x^{-1}\phi^r(x)]_r^p = x^{-1}\phi^{rp}(x),$$

$x \in G_i$ implies

$$x^{-1}\phi^{rp}(x) \in G_{i-1}.$$

Hence we may apply induction to G_{n-1} to conclude that the automorphism

$$\phi_1 = \phi^{p^{n-2}(p^m-1)}$$

leaves G_{n-1} elementwise fixed.

But then

$$(\phi_1(g))^p = \phi_1(g^p) = g^p,$$

whence $\phi_1(g) = gz$, with $z^p = 1$. But then $z \in G_{n-1}$, $\phi_1(z) = z$ and $\phi_1{}^p(g) = g$. It follows that

$$\phi_1^p = \phi^{p^{n-1}(p^m-1)}$$

is the identity on G.

For the second part of the lemma we need the statement:

(40) $$[g]_r^j \in G_{n-1} \quad \text{if and only if } p^q | j.$$

We have proved (40) above for $i = 1$. If $i > 1$, set $g_1 = [g]_r{}^p$. Since g_1 is a generator of G_{n-1} of index rp, it follows by induction that

$$[g_1]_{rp}^k \in G_{n-1}$$

if and only if $p^{i-1} | k$. But now by Lemma 2.1,

$$[g_1]_{rp}^k = [g]_r^{pk},$$

and (40) follows at once.

In particular, (40) implies that

$$[g]_r^{p^n} = 1$$

and that there are exactly $p^n - p^{n-1}$ values of $j < p^n$ for which $[g]_r{}^j$ has order p^n. For these values of j the elements $\phi^t([g]_r{}^j)$ must exhaust the $p^{mn} - p^{m(n-1)}$ elements of G of order p^n. Hence

$$h(p^n - p^{n-1}) \geqslant p^{mn} - p^{m(n-1)}.$$

But $h | p^{n-1}(p^m - 1)$, whence

(41) $$p^{n-1}(p^m - 1)(p^n - p^{n-1}) \geqslant p^{mn} - p^{m(n-1)}.$$

It follows that $p - 1 \geqslant p^{m(n-1)-2n+2}$, and we conclude from this inequality that either $n = 1$ or $m \leqslant 2$.

The following theorem will be of considerable importance in determining the structure of a regular ϕ-group.

THEOREM 6. *Assume that a regular ϕ-group G of index r and order p^n contains a sequence of normal subgroups $G = G_n \supset G_{n-1} \supset \ldots \supset G_1 \supset G_0 = 1$, invariant under ϕ, such that no subgroup of G invariant under ϕ lies properly between G_i and G_{i-1} and such that if $x \in G_i$, $x^{-1}\phi^r(x) \in G_{i-1}$, $i = 1, 2, \ldots, n$. Then G is Abelian.*

Proof. We shall first show that all the elements of order p in G are contained in G_1, and hence that G_1 lies in the centre of G. $\bar{G} = G/G_1$ satisfies all the conditions of the lemma, and hence by induction the elements of order p in $\bar{G}$ are contained in the subgroup $\bar{G}_2 = G_2/G_1$, which is Abelian of type (p, p, . . . , p). Hence the elements of order p in G are contained in G_2. Since G_1 is a minimal subgroup of G invariant under ϕ, it is also Abelian of type (p, p, . . . , p).

We have G_2 of index rs with respect to some generator g_2, $g_2^p \in G_1$, and $\phi^r(g_2) = yg_2$ for some y in G_1. Since G_1 is normal in G_2, it follows directly that

$$[g_2]_{r,s}^j = z_j g_2^j, \qquad z_j \text{ in } G_1.$$

If g_2 has order p^2, we conclude at once from this relation that the elements of order p in G_2 are contained in G_1.

On the other hand, suppose $g_2^p = 1$. First of all, if G_1 were not in the centre C of G_2, we would have $G_1 \cap C = 1$ and $G_1C/G_1 \cong \bar{G}_2$, since no proper subgroup of $\bar{G}_2$ is invariant under ϕ. But then $G_2 = G_1C$, and so G_2 is Abelian. G_1 must therefore lie in the centre of G_2. But now if $\phi^{rs}(g_2) = zg_2$, $z \in G_1$, it follows that

$$[g_2]_{r,s}^j = z^{j(j-1)/2} g_2^j.$$

If p is odd, we conclude that $[g_2]_{r,s}^p = g_2^p = 1$, a contradiction to the fact that G_1 is spanned by the elements of the form

$$\phi^i([g]_{r,s}^{p,j}).$$

If $p = 2$, (42) gives $[g_2]_{r,s}^4 = 1$, and so the orbits of the four elements $[g_2]_{r,s}^j$, $j = 1, 2, 3, 4$ must span G_2. But

$$[g_2]_{r,s}^3 = zg_2 = \phi^{rs}(g_2)$$

since $g_2^2 = 1$, and hence $[g_2]_{r,s}^1$ and $[g_2]_{r,s}^3$ determine the same orbit. It follows that the orbit of g_2 under ϕ must include every element of $G_2 - G_1$, whence

$$h \geqslant o(G_2) - o(G_1). \tag{43}$$

Since our assumptions imply that every element of G_2 is of order 2, G_2 is Albelian and we may regard ϕ as a linear transformation of an n-dimensional vector space ($2^n = o(G_2)$), over the field with 2 elements, which leaves some t-dimensional subspace invariant ($2^t = o(G_1)$). But the maximum order of such a linear transformation is easily computed to be $(2^t - 1)(2^{n-t} - 1)$, which is less than $2^n - 2^t$, in contradiction to (43). Hence G_1 consists of the elements of order dividing p in G, as asserted.

If $o(G_1) = p$, G therefore has a unique subgroup of order p, and as is well-known, this implies that G is either cyclic or isomorphic to the generalized quaternion group of order 2^n. But this last group has a unique element of order 2, which is necessarily fixed by every automorphism of the group.

Hence G is Abelian if G_1 is cyclic. We assume therefore that $o(G_1) = p^t$ with $t \geqslant 2$.

We consider the group $\bar{G} = G/G_1$, and suppose k to be the order of the image $\bar{\phi}$ of ϕ on $\bar{G}$. If F denotes the subgroup of G left elementwise fixed by ϕ^k, we have $F \cap G_1 = 1$ or $F \cap G_1 = G_1$, since G_1 is a minimal subgroup of G invariant under ϕ and since F is also invariant under ϕ. Since G_1 contains every element of order p in G, $F \cap G_1 = 1$ implies $F = 1$.

Consider the case $F = 1$. If g is a generator of G, $\phi^k(g) = z_1 g$, z_1 in G_1; and since ϕ^k leaves only the identity element of G_1 fixed, $z_1 = x^{-1}\phi^k(x)$ for some x in G_1, and $\phi^k(x^{-1}g) = x^{-1}g$. Thus $x^{-1}g \in F$, whence $g = x$. Thus $G = G_1$ is Abelian. We may thus suppose $F \supset G_1$.

Now $\bar{G}$ satisfies all the hypotheses of the theorem and is Abelian by induction. But then it satisfies the conditions of Lemma 6.1, and consequently is either cyclic, of type (p^{n-1}, p^{n-1}) or of type $(p, p, \ldots, p)$ and order p^m with $k | p^m - 1$. If $\bar{G}$ is cyclic, G is of course Abelian, since G_1 is in its centre. In the second case, it follows that every element of G is of the form $xg^i\phi(g)^j$ for some element x in G_1 and suitable integers i, j. Suppose now that

$$\phi(g)g = yg\phi(g), \qquad y \text{ in } G_1. \tag{44}$$

Since $\bar{G}$ is of type (p^{n-1}, p^{n-1}), $\bar{\phi}^2(\bar{g}) = \bar{g}^\alpha \bar{\phi}(\bar{g}^\beta)$ for some integers α, β, where $\bar{g}$ denotes the image of g in $\bar{G}$. Hence

$$\phi^2(g) = zg^\alpha \phi(g^\beta), \qquad z \in G_1. \tag{45}$$

Now apply ϕ to (44) and use (45) to obtain

$$\begin{aligned} \phi^2(g)\phi(g) = \phi(y)\phi(g)\phi^2(g) &= \phi(y)\phi(g)zg^\alpha\phi(g^\beta) \\ &= \phi(y)y^\alpha(zg^\alpha\phi(g^\beta))\phi(g) = \phi(y)y^\alpha\phi^2(g)\phi(g). \end{aligned} \tag{46}$$

Hence $\phi(y) = y^{-\alpha}$, and the subgroup H generated by y is invariant under ϕ. Since $H \subset G_1$, we have $H = G_1$ or $H = 1$. In the first case, $o(G_1) = p$, contrary to our present assumption. Hence $y = 1$ and it follows at once from (44) that G is Abelian.

There remains the case $F \supset G_1$, $\bar{G}$ Abelian of type $(p, p, \ldots, p)$ and order p^m, with $k | p^m - 1$. In this case the relation $\phi^k(g) = z_1 g$ implies $\phi^{kp}(g) = g$, whence

$$h | kp | (p^m - 1)p. \tag{47}$$

On the other hand, as in the proof of Lemma 10.1

$$[g]_r^{p^2} = 1,$$

and hence

$$hp^2 > o(G) = o(G_1)o(\bar{G}) = p^{t+m}. \tag{48}$$

Combining (22) and (23), we get the inequality $(p^m - 1)p^2 > p^{t+m}$, which implies $t < 2$. We are assuming $t > 1$ and hence $t = 2$.

The theorem has already been proved if $m \leqslant 2$. Hence we may assume $m \geqslant 3$. Let $\bar{y}_1, \bar{y}_2, \ldots, \bar{y}_m$ be a basis for $\bar{G}$ and $y_1, y_2, \ldots, y_m$ a set of representatives in G. Since G_1 contains all elements of G of order p, $y_i^p \neq 1$ for all i. Since $y_i^p \in G_1$ and G_1 is of type (p, p), there exists integers γ_1 and γ_2 such that

$$y_3^p = y_1^{p\gamma_1} y_2^{p\gamma_2}. \tag{49}$$

On the other hand, if

$$y_3(y_1^{\gamma_1} y_2^{\gamma_2}) = x_1 y_1^{\gamma_1} y_2^{\gamma_2} y_3 \quad \text{and} \quad y_2^{\gamma_2} y_1^{\gamma_1} = x_2 y_1^{\gamma_1} y_2^{\gamma_2},$$

then

$$(y_3^{-\gamma_2} y_1^{-\gamma_1} y_3)^p = x_1^{p(p+1)/2} (y_3^{-\gamma_2} y_1^{-\gamma_1})^p y_3^p = (x_1 x_2)^{p(p+1)/2} y_2^{-\gamma_2 p} y_1^{-\gamma_1 p} y_3^p. \tag{50}$$

If p is odd, it follows at once from (49) and (50) that $y_2^{-\gamma_2} y_1^{-\gamma_1} y_3$ has order p and hence is in G_1. We conclude that $\bar{y}_3 = \bar{y}_1^{\gamma_1} \bar{y}_2^{\gamma_2}$, which implies $m \leqslant 2$, a contradiction.

On the other hand, if $p = 2$, and $\bar{g}$ is the residue of g in $\bar{G}$, it follows as in the first part of the proof that $[g]_r^4 = 1$, that $[g]_r^3$ and $[g]_r^1$ determine the same orbits, and hence that the orbit of g under ϕ must include all $2^2(2^m - 1)$ elements of $G - G_1$, and hence

$$h \geqslant 2^2(2^m - 1). \tag{51}$$

On the other hand, since every element of G_1 is of the form $\phi^t(g_1^t)$, ϕ has order 3 on G_1. Since $F \supset G_1$, $3|k$. But then $\phi^k(g) = xg$, $x \in G_1$, implies $\phi^{2k}(g) = g$, whence $h|2k$. Since $k \leqslant 2^m - 1$, $h \leqslant 2(2^m - 1)$ in contradiction to (51).

COROLLARY. *A regular ϕ-group of index 0 and of prime power order is Abelian.*

The structure of ϕ-groups of index 0 is now easily obtained.

THEOREM 7. *A regular ϕ-group of index 0 is Abelian.*

Proof. If G is of index 0, so is every one of its subgroups. Since ϕ is regular, ϕ leaves some p-Sylow subgroup of G invariant for every $p|o(G)$. It follows from the preceding corollary that the Sylow subgroups of G are all Abelian. and hence by the corollary of Theorem 1, that G is Abelian.

11. The structure of regular ϕ-groups of prime power order.

THEOREM 8. *A regular ϕ-group of prime power order is either Abelian or metabelian.*

Proof. Let G be a regular ϕ-group of index r and order p. We shall first prove that G contains a normal subgroup F^* invariant under ϕ and of index rs such that

(a) F^* satisfies the hypotheses of Theorem 6.
(b) $\bar{G} = G/F^*$ is Abelian of type $(p, p, \ldots, p)$.
(c) The image $\bar{\phi}^r$ of ϕ^r leaves only the identity element of $\bar{G}$ fixed.
(d) If k = order of $\bar{\phi}$, then $(k, p) = 1$ and $k|rs$.

We shall then show that F^* is actually in the centre of G.

Suppose first that ϕ^r leaves some proper subgroup F of G elementwise fixed. By Theorem 2, F is normal in G. Let $\bar{G} = G/F$. By induction $\bar{G}$ contains a subgroup $\bar{F}^*$ of index rs such that $\bar{F}^*$, $\bar{G} = \bar{G}/\bar{F}^*$, and the image $\bar{\phi}$ of ϕ on $\bar{G}$ satisfy conditions (a) to (d). If F^* denotes the inverse image of $\bar{F}^*$ in G, F^* is of index rs. Since F is of index 0, it follows readily from Lemma 6.1 and condition (a) for $\bar{F}^*$ that F^* satisfies (a). Since $G/F^* \cong \bar{G}$, the remaining conditions follow at once.

We may therefore assume that ϕ^r leaves only the identity element of G fixed. If G is Abelian of type $(p, p, \ldots, p)$ and $(h, p) = 1$, where h = order of ϕ, set $F^* = 1$.

If G is not of this form, let C_1 be a minimal subgroup of the centre of G, invariant under ϕ, and set $\bar{G} = G/C_1$, $\bar{\phi}$ = image of ϕ on $\bar{G}$. If $\bar{G}$ is Abelian of type $(p, p, \ldots, p)$ and the order m of $\bar{\phi}$ is relatively prime to p, we let H be the subgroup of elements of G left elementwise fixed by ϕ^m. If $H \cap C_1 = 1$, it follows by the usual argument that $G = C_1H$, that $H \cong \bar{G}$, and consequently that G is Abelian of type $(p, p, \ldots, p)$. Since C_1 is a minimal subgroup of G invariant under ϕ, the order of ϕ on C_1 is relatively prime to p, and it follows at once that $(h, p) = 1$, a contradiction. Thus $H \supset C_1$.

Let g be a generator of G of index r and $g_1 = [g]_r$ a generator of C_1 of index rs. If $\bar{g}$ is the residue of g in $\bar{G}$, $[\bar{g}]_r = 1$, and since $\bar{\phi}$ leaves only the identity element of $\bar{G}$ fixed, it follows that $\bar{\phi}^{rs}(\bar{g}) = \bar{g}$. Thus $m|rs$. Since $H \supset C_1$ we conclude that $x^{-1}\phi^{rs}(x) = 1$ for all x in C_1. If we put $F^* = C_1$, it is clear that conditions (a) to (d) hold.

Consider then the case in which either $\bar{G}$ is not Abelian of type $(p, p, \ldots, p)$ or $(m, p) \neq 1$ so that $\bar{G}$ contains at least one proper normal subgroup invariant under ϕ. By induction $\bar{G}$ contains a proper normal subgroup $\bar{F}^*$ of index rs such that if $\bar{\bar{G}} = \bar{G}/\bar{F}^*$, $\bar{\bar{\phi}}$ = image of $\bar{\phi}$ on $\bar{\bar{G}}$, and k = order of $\bar{\bar{\phi}}$, then $\bar{F}^*$ satisfies the conditions of Theorem 6, $\bar{\bar{G}}$ is Abelian of type $(p, p, \ldots, p)$, $(k, p) = 1$ and $k|rs$, and $\bar{\bar{\phi}}^r$ is Frobenius. Our conditions imply that $\bar{\bar{\phi}}^{rs}(\bar{\bar{g}}) = \bar{\bar{x}}\bar{\bar{g}}$, $\bar{\bar{x}} \in \bar{F}^*$. It follows as in the derivation of (39) and (40) that

$$\bar{\bar{\phi}}^{rsp^n}(\bar{\bar{g}}) = \bar{\bar{g}}$$

for some integer n, and hence

$$m|rsp^n. \tag{52}$$

Let H be the subgroup of G left elementwise fixed by ϕ^{rsp^n}, and suppose first that $H \supset C_1$. Let F^* be the inverse image of $\bar{F}^*$ in G. The index of F^* = index of $\bar{F}^* = rs$. Furthermore $\phi^{rsp^n}(x) = x$ for all x in C_1. Since C_1 is a minimal subgroup of G invariant under ϕ, the order of ϕ on C_1 is relatively

prime to p, and hence $x^{-1}\phi^{rs}(x) = 1$ for all x in C_1. It follows immediately that F^* satisfies (a). Since $G/F^* \cong \bar{G}/\bar{F}^*$, (b), (c), and (d) also hold.

On the other hand, if $H \cap C_1 = 1$, it follows once again that $G = C_1H$ and that $\bar{G} \cong H$ under an isomorphism τ such that $(\tau\bar{\phi}(\bar{x})) = \phi(\tau(\bar{x}))$ for all $\bar{x}$ in $\bar{G}$. Let F' be the normal subgroup of H which corresponds to $\bar{F}^*$ under τ. Then F' is invariant under ϕ, ϕ has order m on H and $m|rsp$. Let F_1 be a minimal subgroup of F' invariant under ϕ. Since every subgroup of F' invariant under ϕ is characteristic in F', F_1 is normal in H and hence also in G. Let $G' = G/F_1$, $\phi' =$ image of ϕ on G', $m' =$ order of ϕ'. By induction G' contains a normal subgroup F'^* of index rs' such that conditions (a), (b), (c) hold for F'^* and $\bar{G} = G/F'^*$. In particular, $m' = rs'p^{n'}$ for some integer n'. Let H_1 be the subgroup of G invariant under

$$\phi^{rs'p^{n'}}.$$

Since $\bar{F}^*$ is the homomorphic image of C_1F', C_1F' is of index rs. Since $F_1 \subset C_1F'$, it follows that $rs|rs'$, and hence $H_1 \supset F_1$. Our desired conclusion now follows as in the preceding paragraph.

It remains to prove that F^* lies in the centre of G. By construction F^* contains a sequence of normal subgroups $F^* = F_n \supset F_{n-1} \supset \cdots \supset F_1 \supset F_0 = 1$ invariant under ϕ such that

$$x^{-1}\phi^{rs}(x) \in F_{i-1} \text{ if } x \in F_i$$

and such that no proper subgroup of F^* invariant under ϕ lies properly between F_i and F_{i-1}. By Theorem 6, F^* is Abelian. It is easy to see that this implies that F^* is of type $(p^n, p^n, \ldots, p^n)$ and that F_i is the subgroup generated by the elements of order p^i in F^*. Thus F_1 is characteristic in F^*, and consequently normal in G. Since F^* is a minimal subgroup of G invariant under ϕ, we conclude that F_1 lies in the centre of G.

Since $\bar{G}$ is Abelian of type $(p, p, \ldots, p)$ we can decompose $\bar{G}$ into the direct product of subgroups $\bar{G}_j$, $j = 1, 2, \ldots, t$ invariant under $\bar{\phi}^{rs}$ and none of which can be further decomposed into proper subgroups invariant under $\bar{\phi}^{rs}$. If G_j denotes the inverse image of $\bar{G}_j$, it suffices to prove that F^* lies in the centre of each G_j. For definiteness, take $j = 1$.

First of all, if $\bar{\phi}^{rs}$ has non-trivial fixed elements on $\bar{G}_1$, it follows from the minimality of $\bar{G}_1$ that $\bar{\phi}^{rs}$ is in fact the identity on $\bar{G}_1$. Hence if $x \in G_1$, $x^{-1}\phi^{rs}(x) \in F^*$. It follows at once that G_1 is a group of index rs satisfying the conditions of Theorem 6, and hence is Abelian. Thus F^* is in the centre of G_1 in this case.

Consider then the case in which $\bar{\phi}^{rs}$ leaves only the identity element of $\bar{G}_1$ fixed. $\bar{G}_1$ has a basis $\bar{y}_1, \ldots, \bar{y}_q$ such that

$$\bar{\phi}^{rs}(\bar{y}_i) = \bar{y}_{i+1}, \qquad i = 1, 2, \ldots, q-1$$

and

$$\bar{\phi}^{rs}(\bar{y}_q) = \bar{y}_1^{\alpha_1}\bar{y}_2^{\alpha_2}\cdots\bar{y}_q^{\alpha_q} \tag{53}$$

for suitable integers $\alpha_1, \alpha_2, \ldots, \alpha_q$.

If

$$\bar{y}_1^{i_1}\bar{y}_2^{i_2}\dots\bar{y}_q^{i_q}$$

is a fixed element of $\bar{\phi}^{rs}$, then it is easily checked that the integers $i_1, i_2, \dots, i_q$ are a solution of the congruences.

$$\alpha_1 i_q \equiv i_1; \alpha_2 i_q + i_1 \equiv i_2; \dots; \alpha_q i_q + i_{q-1} \equiv i_q \pmod{p}, \tag{54}$$

and conversely. It follows readily from (54) that ϕ^{rs} is Frobenius on $\bar{G}_1$ if and only if

$$(\alpha_1 + \alpha_2 + \dots + \alpha_q - 1, p) = 1. \tag{55}$$

Let y_i be a representative of $\bar{y}_i$ in G_1 such that

$$\phi^{rs}(y_i) = y_{i+1}, \qquad i = 1, 2, \dots, q-1.$$

Then

$$\phi^{rs}(y_q) = x_0 y_1^{\alpha_1} y_2^{\alpha_2} \dots y_q^{\alpha_q},$$

$x_0 \in F^*$. If ψ denotes the automorphism of F^* induced by conjugation by y_1, ψ leaves F_1 elementwise fixed since F_1 lies in the centre of G_1. We shall prove by induction on n that ψ leaves F^* elementwise fixed. This will suffice to prove that F^* is in the centre of G_1, and will complete the proof of the theorem.

By induction F^*/F_1 lies in the centre of G/F_1, whence

$$\text{if } x \in F^*, \quad \psi(x) = zx, \quad z \in F_1. \tag{56}$$

Suppose ψ is the identity on F_k with $1 \leqslant k < n$. We shall prove ψ is the identity on F_{k+1}. Applying ϕ^{rsi} to (56), we obtain

$$\phi^{rsi}(\psi(x)) = \phi^{rsi}(y_1)\phi^{rsi}(x)\phi^{rsi}(y_1^{-1}) = \phi^{rsi}(z)\phi^{rsi}(x) = z\phi^{rsi}(x). \tag{57}$$

But if $x \in F_{k+1}$, $\phi^{rsi}(x) = xz_i$, $z_i \in F_k$. Since F_k is in the centre of G_1, we conclude from (57) that

$$\phi^{rsi}(\psi(x)) = zx = \psi(x) \quad \text{for all } i \text{ and all } x \text{ in } F_{k+1}. \tag{58}$$

By repeated use of (58) we now obtain

$$\psi(x) = \phi^{rsq}(\psi(x)) = (x_0 y_1^{\alpha_1} y_2^{\alpha_2} \dots y_q^{\alpha_q})(x)(x_0 y_1^{\alpha_1} y_2^{\alpha_2} \dots y_q^{\alpha_q})^{-1} = \psi^{\alpha_1+\alpha_2+\dots+\alpha_q}(x),$$

whence

$$\psi^{\alpha_1+\alpha_2+\dots+\alpha_{q-1}}(x) = x, \qquad x \in F_{k+1}. \tag{59}$$

On the other hand, (56) implies $\psi^p(x) = x$. But then (55) and (59) together imply $\psi(x) = x$ for all k in F_{k+1}. Q.E.D.

Theorem 8 and Theorem 4 together imply

THEOREM 9. *A regular ϕ-group is either Abelian or nilpotent of class 2.*

We conjecture that a regular ϕ-group is Abelian if ϕ^r is Frobenius. This result would follow easily from the following conjecture concerning fixed-point free automorphisms of p-groups.

CONJECTURE. *Let G be a non-Abelian p-group which admits an automorphism ϕ of order h leaving only the identity element of G fixed, and assume that G cannot be expressed as the direct product of two proper subgroups invariant under ϕ. Then $h^2 < o(G)$.*

12. The relation between ϕ-groups and groups of the form ABA. In the proof of the preceding theorem we have already seen that a ϕ-group G can be imbedded as a normal subgroup of an ABA-group G^* satisfying $G^* = GA$ and $G \cap A = 1$. The converse is also true, and consequently we have

THEOREM 10. *G is a ϕ-group if and only if it can be imbedded as a normal subgroup of a group G^* of the form ABA, where A and B are cyclic subgroups of G^*, such that $G^* = GA$ and $A \cap G = 1$.*

Proof. It suffices to prove that if an ABA-group G^* in which A, B are cyclic contains a normal subgroup G such that $G^* = GA$ and $G \cap A = 1$, then G is a ϕ-group.

If a, b are generators of A, B respectively, we have $b = ga^r$ for some element g in G and some integer r. Since G is normal, the elements

$$b^j a^{-jr} = (ba^{-r})(a^r ba^{-2r}) \cdots (a^{(j-1)r} ba^{-jr}) = g(a^r ga^{-r}) \cdots a^{(j-1)r} ga^{-(j-1)r} \tag{60}$$

are in G for all i, j.

Suppose for some j, $b^j a^k \in G$; then $a^{-k-jr} = (b^j a^k)^{-1}(b^j a^{-jr}) \in G \cap A$. Since $G \cap A = 1$, $a^k = a^{-jr}$. It follows at once that G consists precisely of the elements of G^* of the form $a^i b^j a^{-jr-i}$. If we now define ϕ to be an automorphism of G induced by conjugation by a, it follows as in the proof of Theorem 5 that every element of G is of the form $\phi^i([g]_r{}^j)$. Thus G is a ϕ-group of index r and with generator g.

Combining Theorems 5 and 10, we obtain our final result:

THEOREM 11. *A group G^* which is of the form ABA, where A and B are cyclic subgroups, and which contains a normal subgroup G such that $G^* = GA$ and $G \cap A = 1$ is solvable.*

In a subsequent paper we shall show that an ABA group G^* with a trivial centre in which A is its own normalizer and A is of odd order always contains a normal subgroup G such that $G^* = GA$ and $G \cap A = 1$. We shall also determine the structure of G^* when $o(A)$ is even and, in particular, shall show that G^* is solvable.

References

1. W. Burnside, *Theory of groups of finite order* (Dover, New York, 1955).
2. W. Feit, *On the structure of Frobenius groups*, Can. J. Math., *9* (1957), 587–96.
3. D. Gorenstein, *A class of Frobenius groups*, Can. J. Math., *11* (1959), 39–42.
4. D. Gorenstein and I. N. Herstein, *A class of solvable groups*, Can. J. Math., *11* (1959), 311–20.
5. G. Higman, *Groups and rings which have automorphisms without non-trivial fixed elements*, J. London Math. Soc., *32* (1957), 321–334.
6. H. Zassenhaus, *The theory of groups* (Chelsea, New York, 1958).

Clark University

SUR LE RADICAL CORPOÏDAL D'UN ANNEAU

G. THIERRIN

Le radical d'un anneau, dans le sens général de N. Jacobson **(1; 2)**, peut être caractérisé de plusieurs manières. On peut, par exemple, le définir comme l'intersection de tous les idéaux primitifs de l'anneau envisagé. Dans ce travail, nous considérons une classe particulière d'idéaux primitifs, la classe des idéaux corpoïdaux: un idéal est dit corpoïdal si et seulement si l'anneau-quotient correspondant est un corps.[1] L'objet principal de ce travail est de donner quelques caractérisations de l'intersection C de tous les idéaux corpoïdaux d'un anneau A, intersection appelée le radical corpoïdal de l'anneau A. Si C est distinct de A,. l'anneau-quotient A/C est isomorphe à une somme sous-directe de corps Dans le cas d'un anneau commutatif, tout idéal primitif est corpoïdal, et par conséquent son radical corpoïdal coïncide avec son radical.[2]

1. Anneaux et modules interversifs. Un anneau A est dit *interversif à droite*, si l'on a

$$abA = baA, \text{ quels que soient } a, b \in A.$$

Un idéal H d'un anneau A est dit *interversif à droite*, si l'anneau-quotient A/H est interversif à droite. On voit facilement qu'un idéal H est interversif à droite, si et seulement si pour tout triple $a, b, c \in A$, il existe $x \in A$ tel que l'on ait

$$abc \equiv bax \quad (H).$$

Il s'ensuit que tout idéal contenant un idéal interversif à droite est interversif à droite. En particulier, tout idéal d'un anneau interversif à droite est interversif à droite.

Rappelons qu'un anneau A est dit *réflecteur à droite*, si, pour tout idéal à droite H de A, la relation $ab \in H$ entraîne $ba \in H$ **(3)**.

THÉORÈME 1. *Pour qu'un anneau A possédant un élément unité soit interversif à droite, il faut et il suffit qu'il soit réflecteur à droite.*

La condition est nécessaire. Si $ab \in H$, où H est un idéal à droite de A, on a $abA = baA \subseteq H$. D'où $ba \in H$.

La condition est suffisante. Soient $a, b, c \in A$. L'anneau A étant réflecteur à droite et possédant un élément unité, il existe, d'après **(3)**, un élément x tel

Reçu le 15 Décembre, 1958.

[1] Par corps, nous entendons un anneau dont l'ensemble des éléments distincts de zéro forme un groupe pour la multiplication.

[2] La nomenclature de ce travail est celle de N. Jacobson **(1)**.

que l'on ait $ab = bax$. Par conséquent, $abc = baxc$ et l'idéal (0) est interversif à droite.

Remarquons que tout idéal à droite d'un anneau interversif à droite possédant un élément unité est un idéal bilatère.

Un A-module[3] M est dit *interversif*, si l'on a

$$uabA = ubaA, \text{ quels que soient } u \in M, a, b \in A.$$

Si l'anneau A est interversif à droite, tout A-module est évidemment interversif.

THÉORÈME 2. *Pour qu'un anneau A soit un corps, il faut et il suffit qu'il existe un A-module M irréductible, fidèle et interversif.*

La condition est nécessaire. En effet, il suffit de prendre $M = A$.

La condition est suffisante. Le A-module M étant irréductible, si $0 \neq u \in M$, on a, d'après **(1**, ch. I**)**, $M = uA \cong A - (0 : u)$, où $(0 : u) = J$ est un idéal à droite modulaire maximal. Soient $t \in J$ et $x \in A$; on a $txA \subseteq J$ et $utxA = uxtA = 0$. D'où $xtA \subseteq J$. L'ensemble

$$J^{\cdot}.A = \{a | a \in A, aA \subseteq J\}$$

est un idéal à droite de A et $J \subseteq J^{\cdot}.A$. On a donc soit $J^{\cdot}.A = J$, soit $J^{\cdot}.A = A$. Si $J^{\cdot}.A = A$, on a $A^2 \subseteq J$, ce qui est impossible puisque J est modulaire. Par conséquent $J^{\cdot}.A = J$. Comme $xt \in J^{\cdot}.A$, on a $xt \in J$ et donc J est un idéal bilatère. Soit $N = \{v | v \in M, vJ = 0\}$. Cet ensemble N est un sous-module de M et $u \in N$. Donc $N \neq 0$ et, puisque M est irréductible, $N = M$, ce qui entraîne $J \subseteq (0 : M)$. Comme M est fidèle, on a $(0 : M) = 0$. Par conséquent, $J = 0$ et A est un corps.

COROLLAIRE. *Pour qu'un anneau A soit un corps, il faut et il suffit qu'il soit primitif et interversif à droite.*

La condition est évidemment nécessaire. Elle est suffisante. En effet, l'anneau A étant primitif, il existe un A-module M irréductible et fidèle. Comme A est interversif à droite, le module M est interversif, et donc A est un corps, d'après le théorème.

Un idéal K d'un anneau A est dit *corpoïdal*, si l'anneau-quotient A/K est un corps. On voit facilement qu'un idéal est corpoïdal, si et seulement s'il est un idéal à droite modulaire maximal.

THÉORÈME 3. *Pour qu'un idéal K d'un anneau A soit corpoïdal, il faut et il suffit qu'il existe un A-module M irréductible et interversif, tel que l'on ait $K = (0 : M)$.*

La condition est nécessaire. L'anneau-quotient A/K étant un corps, il existe, d'après le théorème 2, un A/K-module M irréductible, fidèle et interversif. Mais ce A/K-module M peut aussi être considéré comme un A-module.

[3]Dans ce travail, le terme "module" signifie toujours module à droite.

Le A-module M est également irréductible et l'on a $K = (0 : M)$. Montrons que le A-module M est interversif. Soient $a, b \in A$ et $u \in M$. Si $u = 0$, on a évidemment $uabA = ubaA = 0$. Soit $u \neq 0$. Si $ab \in K$, alors $ba \in K$. De $abA \subseteq K$ et $baA \subseteq K$ suit $uabA = ubaA = 0$. Si $ab \notin K$, alors $ba \notin K$, $abA \not\subset K$ et $baA \not\subset K$. Comme K est un idéal à droite maximal, on a

$$A = K + abA = K + baA.$$

L'élément u étant différent de zéro, on a, puisque M est un A-module irréductible, $uA = M$. D'où

$$uA = uK + uabA = uK + ubaA = M.$$

Comme $uK = 0$, on a par conséquent

$$uabA = ubaA = M.$$

La condition est suffisante. En effet, M peut être considéré comme un A/K-module irréductible et fidèle, car on a $K = (0 : M)$ et M est un A-module irréductible. On voit d'autre part facilement que M, considéré comme A/K-module, est aussi interversif. Parconséquent l'anneau-quotient A/K est, d'après le théorème 2, un corps.

2. Radical corpoïdal. Soient A un anneau quelconque et $\sum$ l'ensemble des A-modules M_t irréductibles et interversifs. Le noyau C de $\sum$, c'est-à-dire l'ensemble $C = \bigcap\{(0 : M_t) | M_t \in \sum\}$ est appelé le *radical corpoïdal* de A. Si $\sum$ est vide, le radical corpoïdal de A est, par définition, A lui-même.

Si R est le radical[4] de A, $R \subseteq C$. Si A est interversif à droite, $R = C$.

THÉORÈME 4. *S'il est distinct de A, le radical corpoïdal C d'un anneau A est l'intersection des idéaux corpoïdaux de A.*

C'est immédiat, d'après le théorème 3.

Un anneau A est dit *c-semi-simple*, si $A \neq 0$ et si le radical corpoïdal de A se réduit à 0.

THÉORÈME 5. *Si le radical corpoïdal C de l'anneau A est distinct de A, l'anneau-quotient A/C est c-semi-simple.*

L'intersection des idéaux corpoïdaux de A étant C d'après le théorème 4, il s'ensuit facilement que l'intersection des idéaux corpoïdaux de A/C se réduit à zéro. Donc A/C est c-semi-simple.

THÉORÈME 6. *Un anneau A est isomorphe à une somme sous-directe de corps, si et seulement s'il est c-semi-simple.*

Si A est c-semi-simple, l'idéal (0) est l'intersection des idéaux corpoïdaux K_t de A. Par conséquent, A est isomorphe à une somme sous-directe des

[4]Les notions de radical et de semi-simplicité d'un anneau sont, dans ce travail, prises dans le sens général de Jacobson **(1, 2)**.

anneaux-quotients A/K_t qui sont des corps. Inversement, il est immédiat que si A est isomorphe à une somme sous-directe de corps, A est c-semi-simple.

3. Eléments c-quasi-réguliers. Si a est un élément fixé d'un anneau A, on désigne d'après Jacobson **(1)** (même si A ne contient pas d'élément unité) par $(1 - a)A$ l'idéal à droite $\{x - ax | x \in A\}$ et par $A(1 - a)$ l'idéal à gauche $\{x - xa | x \in A\}$.

Un élément z de A est dit *c-quasi-régulier*, si l'idéal à droite $(1 - z)A$ n'est contenu dans aucun idéal corpoïdal de A.

THÉORÈME 7. *Un élément z de A est c-quasi-régulier si et seulement si l'idéal à gauche $A(1 - z)$ n'est contenu dans aucun idéal corpoïdal de A.*

La démonstration de ce théorème découle immédiatement du lemme suivant:

LEMME 1. *Si K est un idéal corpoïdal de l'anneau A, les relations $x - ax \in K$ et $x - xa \in K$ sont équivalentes.*

Montrons par exemple que $x - ax \in K$ entraîne $x - xa \in K$. Si $x \in K$, c'est immédiat. Si $x \notin K$, il existe, puisque K est corpoïdal, des éléments e et x' tels que $ye \equiv y(K)$ pour tout $y \in A$ et $xx' \equiv e(K)$. De $x - ax \in K$ suit $x \equiv ax(K)$, $xx' \equiv axx'(K)$, $e \equiv ae \equiv a(K)$. D'où $x \equiv xe \equiv xa(K)$, c'est-à-dire $x - xa \in K$.

Remarquons que tout élément quasi-régulier à droite ou à gauche est c-quasi-régulier.

THÉORÈME 8. *Un élément z de A est c-quasi-régulier si et seulement si l'idéal A est le seul idéal interversif à droite contenant $(1 - z)A$.*

Supposons que z soit c-quasi-régulier. S'il existe un idéal interversif à droite H différent de A contenant $(1 - z)A$, cet idéal H est modulaire, donc contenu dans un idéal à droite (modulaire) maximal J. L'idéal $P = J : A = \{a | a \in A, Aa \subseteq J\}$ est primitif et $H \subseteq P$. Comme H est interversif à droite, P l'est également. Par conséquent, l'anneau-quotient A/P est primitif et interversif à droite, donc un corps d'après le corollaire du théorème 2. L'idéal P est par suite corpoïdal et contient $(1 - z)A$, contre l'hypothèse. Inversement, il est immédiat que si A est le seul idéal interversif à droite contenant $(1 - z)A$, il n'existe pas d'idéal corpoïdal contenant $(1 - z)A$, car tout idéal corpoïdal est interversif à droite.

Un idéal à droite de A est dit *c-quasi-régulier*, si tous ses éléments sont c-quasi-réguliers.

THÉORÈME 9. *Le radical corpoïdal C d'un anneau A est un idéal c-quasi-régulier, contenant tout idéal à droite c-quasi-régulier.*

Soit $z \in C$. Si z n'est pas c-quasi-régulier, $(1 - z)A$ est contenu dans un

idéal corpoïdal K. D'après le théorème 4, $z \in K$. Si x est un élément quelconque de A, on a $x - zx \in K$ et donc $x \in K$. D'où $K = A$, ce qui est impossible. Par conséquent, tout élément de C est c-quasi-régulier.

Soit T un idéal à droite c-quasi-régulier et soit $z \in T$. L'élément zx est c-quasi-régulier pour tout $x \in A$. Si $z \notin C$, il existe un A-module M irréductible et interversif tel que $z \notin (0 : M)$. Posons $K = (0 : M)$; K est un idéal corpoïdal d'après le théorème 3. Il existe $u \in M$, tel que $uz \neq 0$ et l'on a $uzA = M$, puisque M est irréductible. Par conséquent, il existe $a \in A$ tel que $uza = u$. L'élément za étant c-quasi-régulier, on a donc $(1 - za)A \not\subseteq K$. L'idéal K est un idéal à droite maximal; d'où $(1 - za)A + K = A$. Il existe donc $x \in A$ et $k \in K$ tel que l'on ait $x - zax + k = -za$, c'est-à-dire $za + x - zax = -k \in K$. On a d'autre part $0 = u - uza - (u - uza)x = u - u(za + x - zax) = u + uk$. De $k \in K$ suit $uk = 0$ et donc $u = 0$, ce qui est impossible, puisque $uz \neq 0$. Par conséquent, $z \in C$ et $T \subseteq C$.

4. Noyau d'interversion. Un complexe[5] H d'un anneau quelconque A est dit un *complexe d'interversion à droite*, si l'on a $abH = baH$, quels que soient $a, b \in A$. L'élément zéro est un complexe d'interversion à droite. Tout idéal à droite minimal D, qui est un idéal bilatère, est un complexe d'interversion à droite; cela découle du fait que l'on a alors $xD = 0$ ou $xD = D$, pour tout $x \in A$.

On voit facilement qu'un complexe H est un complexe d'interversion à droite, si et seulement si pour tout couple $a, b \in A$ et tout $h \in H$, il existe $h' \in H$ tel que l'on ait $abh = bah'$.

La réunion T de tous les complexes d'interversion à droite de A est appelée le *noyau d'interversion à droite* de A.

THÉORÈME 10. *Si H et K sont des complexes d'interversion à droite de l'anneau A, les complexes HA, AH, $H^* = \{-h/h \in H\}$ et $H + K = \{h + k | h \in H, k \in K\}$ sont des complexes d'interversion à droite.*

De $abH = baH$, quels que soient $a, b \in A$, suit $abHA = baHA$. Donc HA est un complexe d'interversion à droite.

Soit ensuite $vh \in AH$, avec $v \in A$, $h \in H$. Il existe $h' \in H$ tel que $abvh = bvah'$ et $h'' \in H$ tel que $vah' = avh''$. D'où $abvh = bvah' = bavh''$, avec $vh'' \in AH$. Par conséquent, AH est un complexe d'interversion à droite.

Le complexe H^* est un complexe d'interversion à droite, car, si $h \in H$, il existe $h' \in H$ tel que $abh = bah'$; d'où $ab(-h) = ba(-h')$. Montrons enfin que $H + K$ est un complexe d'interversion à droite. Si $h \in H$, $k \in K$, il existe $h' \in H$, $k' \in K$ tels que $abh = bah'$ et $abk = bak'$. D'où $ab(h + k) = ba(h' + k')$.

THÉORÈME 11. *Le noyau T d'interversion à droite d'un anneau A est un*

[5] Par complexe d'un anneau A, nous entendons toute partie non vide de A.

complexe d'interversion à droite, un idéal bilatère et un anneau interversif à droite.

Soient $a, b \in A$ et $t \in T$. Il existe un complexe d'interversion à droite H contenant l'élément t. Par conséquent, il existe $t' \in H \subseteq T$ tel que $abt = bat'$, ce qui montre que T est un complexe d'interversion à droite.

Soient $x, y \in T$. Du théorème 10 et du fait que T est un complexe d'interversion à droite contenant tous les complexes d'interversion à droite de A, on déduit que $-y \in T$ et $x - y \in T$, ce qui montre que T est un sous-groupe additif. Les complexes AT et TA étant, d'après le théorème 10, des complexes d'interversion à droite, on a donc $AT \subseteq T$ et $TA \subseteq T$. Par conséquent, T est un idéal bilatère.

Il est immédiat que T est un anneau interversif à droite.

THÉORÈME 12. *Si R est le radical et T le noyau d'interversion à droite d'un anneau A, le radical corpoïdal de l'anneau T est l'ensemble $T \cap R$.*

Le noyau T étant un idéal bilatère, son radical est, d'après Jacobson (**1**, ch. I), l'ensemble $T \cap R$. Comme T est un anneau interversif à droite, son radical corpoïdal coïncide avec son radical.

COROLLAIRE. *S'il est distinct de zéro, le noyau d'interversion à droite d'un anneau semi-simple est isomorphe à une somme sous-directe de corps.*

BIBLIOGRAPHIE

1. N. Jacobson, *Structure of rings*, Amer. Math. Soc. Coll. Pub., **37**, 1956.
2. ——— *The radical and semi-simplicity for arbitrary rings*, Amer. J. Math., *67* (1945), 300–320.
3. G. Thierrin, *Contribution à la théorie des anneaux et des demi-groupes*, Comm. Math. Helv., *32* (1957), 93–112.

Université de Montréal

ON REPRESENTATIONS OF ORDERS OVER DEDEKIND DOMAINS

D. G. HIGMAN

We study representations of $\mathfrak{o}$-*orders* $\mathfrak{O}$, that is, of $\mathfrak{o}$-regular $\mathfrak{O}$-algebras, in the case that $\mathfrak{o}$ is a Dedekind domain. Our main concern is with those $\mathfrak{O}$-modules, called $\mathfrak{O}$-*representation modules*, which are regular as $\mathfrak{o}$-modules. For any $\mathfrak{O}$-module M we denote by $D(M)$ the ideal consisting of the elements $x \in \mathfrak{o}$ such that $x \cdot \mathrm{Ext}^1(M, N) = 0$ for all $\mathfrak{O}$-modules N, where $\mathrm{Ext} = \mathrm{Ext}_{(\mathfrak{O},\mathfrak{o})}$ is the relative functor of Hochschild **(5)**. To compute $D(M)$ we need the small amount of homological algebra presented in § 1. In § 2 we show that the $\mathfrak{O}$-representation modules with rational hulls isomorphic to direct sums of right ideal components of the rational hull A of $\mathfrak{O}$, called *principal* $\mathfrak{O}$-modules, are characterized by the property that $D(M) \neq 0$. The $(\mathfrak{O}, \mathfrak{o})$-projective $\mathfrak{O}$-modules are those with $D(M) = \mathfrak{o}$. We observe that $D(M)$ divides the ideal $I(\mathfrak{O})$ of **(2)** for every M, and give another proof of the fact that $I(\mathfrak{O}) \neq 0$ if and only if A is separable. Up to this point, $\mathfrak{o}$ can be taken to be an arbitrary integral domain.

The results of the remaining sections are largely generalizations of Maranda's results for groups **(6, 7)**. In §§ 3-5 ew assume that $\mathfrak{o}$ is a local domain with prime ideal $\mathfrak{p}$, and define the *depth* of an $\mathfrak{O}$-module M to be s or ∞ according as $D(M) = \mathfrak{p}^s$ or 0. In § 3 we generalize Maranda's Theorem 2 of **(6)** by proving that an $\mathfrak{O}$-representation module M of depth s is isomorphic with an $\mathfrak{O}$-representation module N if and only if $M/\mathfrak{p}^{s+1}M$ and $N/\mathfrak{p}^{s+1}N$ are isomorphic. In § 4 it is proved, among other things, that for complete $\mathfrak{o}$, an $\mathfrak{O}$-representation module M has depth s if and only if $M/\mathfrak{p}^{s+1}M$ has depth s. This implies, for example, that M is $(\mathfrak{O}, \mathfrak{o})$-projective if and only if $M/\mathfrak{p}M$ is $(\mathfrak{O}/\mathfrak{p}\mathfrak{O}, \mathfrak{o}/\mathfrak{p})$-projective, a slight improvement of a result of Reiner **(8)**, since the "only if" part does not require a special hypothesis. In § 5, $\mathfrak{o}$ is assumed complete, and the $(\mathfrak{O}, \mathfrak{o})$-projective $\mathfrak{O}$-representation modules are characterized as being isomorphic with direct sums of indecomposable right ideal components of $\mathfrak{O}$. A generalization of Maranda's Theorem 4 of **(7)** states that if $I(\mathfrak{O}/\mathfrak{R}) = \mathfrak{o}$, two $(\mathfrak{O}, \mathfrak{o})$-projective $\mathfrak{O}$-representation modules are isomorphic if and only if their rational hulls are isomorphic. Here $\mathfrak{R}$ is the intersection of $\mathfrak{O}$ with the radical of A.

In the final § 6 we apply the local results to the case of a general Dedekind domain $\mathfrak{o}$, observing that for a principal $\mathfrak{O}$-module M, $D(M) = \Pi_{\mathfrak{p}}\mathfrak{p}^s$, where the product is over all primes $\mathfrak{p}$ of $\mathfrak{o}$, and s is the depth of M in the $\mathfrak{p}$-adic completion of $\mathfrak{o}$. We denote by S_M a complete set of non-isomorphic $\mathfrak{O}$-repre-

Received August 26, 1957; in revised form May 21, 1959.

sentation modules N with rational hulls isomorphic to that of M, and such that $D(N) = D(M)$. Although simple examples show that there may be infinitely many non-isomorphic $\mathfrak{O}$-representation modules with rational hulls isomorphic to a given indecomposable right ideal component of A, it seems possible that the cardinal $r(M)$ of S_M, which we call the *class number* of M, is finite if the class number h of $\mathfrak{o}$ is finite. As was pointed out in **(2)**, Maranda's method for the group case **(7)** can be extended to prove this if A is separable and the rational hull of M is absolutely irreducible. Two members of S_M are placed in the same *genus* if they are isomorphic in the $\mathfrak{p}$-adic completion of $\mathfrak{o}$ for all primes $\mathfrak{p}$ of $\mathfrak{o}$. We denote the number of genera in S_M by $g(M)$, and the number of classes in S_M under isomorphism in the $\mathfrak{p}$-adic completion of $\mathfrak{o}$ by $r_\mathfrak{p}(M)$. The final result of this paper is that $g(M) \leqslant \Pi r_\mathfrak{p}(M)$, the product extending over the prime divisors of $D(M) \cap I(\mathfrak{O}/\mathfrak{R})$, with the consequence that $g(M)$ is finite when $\mathfrak{o}$ has finite residue class rings.

1. The ideals $D(M)$ and $C(M)$. We need a small amount of homological algebra. For the basic notations and definitions of this subject we refer the reader to **(1** and **5)**. Throughout this paper, rings will be assumed to have identity elements, identity elements of rings and subrings will be assumed to coincide, and modules will be right unitary unless otherwise specified.

Let Q be a K-subalgebra of a K-algebra P, where K is a commutative ring with identity element. For a P-module M, we define ideals $D(M) = D_{(P,Q)}(M)$ and $C(M) = C_{(P,Q)}(M)$ by

$$D(M) = \{x \in K | x \cdot \mathrm{Ext}^1(M, N) = 0 \text{ for all } P\text{-modules } N\}$$

and

$$C(M) = \{x \in K | x \cdot \mathrm{Ext}^1(N, M) = 0 \text{ for all } P\text{-modules } N\},$$

where $\mathrm{Ext} = \mathrm{Ext}_{(P,Q)}$ is the relative functor introduced by Hochschild **(5)**. According to **(5)**, M is (P, Q)-projective (injective) if and only if $\mathrm{Ext}^1(M, N) = 0$ ($\mathrm{Ext}^1(N, M) = 0$) for all P-modules N, hence

LEMMA 1. *$D(M) = K$, ($C(M) = K$) if and only if M is, (P, Q)-projective (injective).*

The result we use for computing $D(M)$ in the applications to orders is the following.

LEMMA 2. *An element $x \in K$ belongs to $D(M)$ if and only if there exists a P-homomorphism $\beta : M \to M \otimes_Q P$ such that $\beta\tau = x \cdot I_M$, where $\tau : M \otimes_Q P \to M$ is the natural homomorphism, and I_M is the identity map of M.*

Before proving this we recall that $\mathrm{Ext}^1(M, N)$ can be computed as the first cohomology group of the K-complex $\mathrm{Hom}_P(X, N)$ where X is the left P-complex determined by the standard (P, Q)-projective resolution of M. This resolution is the (P, Q)-exact sequence

$$\ldots \xrightarrow{\chi_1} K_1 \otimes_Q P \xrightarrow{\chi_0} M \otimes_Q P \to 0$$

obtained by composing the natural (P, Q)-exact sequences

$$0 \to K_1 \xrightarrow{\eta_1} M \otimes_Q P \xrightarrow{\tau} M \to 0, 0 \to K_2 \xrightarrow{\eta_2} K_1 \otimes_Q P \xrightarrow{\tau_1} K_1 \to 0 \ldots .$$

In particular, $\chi_1 = \tau_2\eta_2$, so $\chi_1\tau_1 = 0$, and hence τ_1 is a 1-cocycle for $\mathrm{Hom}_P(X, K_1)$.

We shall now prove the following lemma, and then derive Lemma 2 as a Corollary.

LEMMA 3.

$$D(M) = \{x \in K | x \cdot \mathrm{Ext}^1(M, K_1) = 0\}$$
$$= \{x \in K | x \cdot \tau_1 \text{ is a coboundary}\}.$$

Proof. For $\alpha \geqslant 0$, $K_\alpha \otimes_Q P$ is (P, Q)-projective, hence there corresponds to each $g \in \mathrm{Hom}_P(K_\alpha \otimes_Q P, K_1)$ an element $g' \in \mathrm{Hom}_P(K_\alpha \otimes_Q P, K_1 \otimes_Q P)$ such that $g'\tau_1 = g$. If $g'\tau_1 = 0$, then $\mathrm{Im}\, g' \subseteq \mathrm{Ker}\tau_1 = \mathrm{Im}\chi_2$. Hence for a 1-cocycle f of $\mathrm{Hom}_P(X, N)$, N a P-module, we have $g'f = 0$. Therefore mapping g onto $g'f$ defines a map $\mu_{f,\alpha} : \mathrm{Hom}_P(K_\alpha \otimes_Q P, K_1) \to \mathrm{Hom}_P(K_\alpha \otimes_Q P, N)$. These maps are readily seen to define a K-map $\mathrm{Hom}_P(X, K_1) \to \mathrm{Hom}_P(X, N)$. Since $\tau_1\tau_1' = 0$, $\mu_{f,\alpha}(\tau f) = f$. Since f can be taken as an arbitrary 1-cocycle of $\mathrm{Hom}_P(X, N)$, the lemma follows.

Proof of Lemma 2. For P-modules A and B, we shall denote by * the natural K-isomorphism $\mathrm{Hom}_Q(A, B) \approx \mathrm{Hom}_P(A \otimes_Q P, B)$.

Let

$$0 \to M \xrightarrow{\kappa} M \otimes_Q P \xrightarrow{\pi} K_1 \to 0$$

be a Q-homotopy for the sequence

$$0 \to K_1 \xrightarrow{\eta} M \otimes_Q P \xrightarrow{\tau} M \to 0,$$

κ being the natural homomorphism.

If now $x \in D(M)$, there exists by Lemma 3 an element $g \in \mathrm{Hom}_P(M, K_1)$ such that $x \cdot \tau = \chi_0 g^*$. Then, since κ^* is the identity map of $M \otimes_Q P$, and $(g\eta)^* = g^*\eta$,

$$0 = [x \cdot \tau - \chi_0 g^*]\eta = x\tau\eta - \chi_0 g^*\eta = \chi_0[x\kappa^* - g^*\eta] = \chi_0[(x \cdot \kappa) - (g\eta)]^*.$$

It follows that $\beta = x \cdot \kappa - g\eta$ is an element of $\mathrm{Hom}_P(M, M \otimes_Q P)$. Further, $\beta\tau = [(x \cdot \kappa\tau) - g\eta\tau] = x \cdot I_M$.

On the other hand, suppose such a β exists. Let $g = [x \cdot \kappa - \beta]\pi \in \mathrm{Hom}_Q(M, K_1)$. Since $[x \cdot \kappa - \beta]\tau = 0$, $g\eta = x \cdot \kappa - \beta$. Further, $\chi_0\beta^* = \chi_0\tau\beta = 0$. Hence

$$\chi_0 g^*\eta = \chi_0(g\eta)^* = \chi_0[x \cdot \kappa^* - \beta^*] = (x \cdot \tau)\eta,$$

so that $\chi_0 g^* = x \cdot \tau$ and $x \in D(M)$ by Lemma 3.

The result corresponding to Lemma 2 for $C(M)$ is

LEMMA 2′. *An element $x \in K$ belongs to $C(M)$ if and only if there exists a P-homomorphism $\gamma \in \mathrm{Hom}_P(\mathrm{Hom}_Q(P, M), M)$ such that $\xi\gamma = x \cdot I_M$, where $\xi : M \to \mathrm{Hom}_Q(P, M)$ is the natural homomorphism.*

This can be proved in the same way as Lemma 2 by first proving the result corresponding to Lemma 3, using the standard (P, Q)-injective resolution of M in place of the projective one. In the following when we state a property of $C(M)$ we shall omit the proof if it is similar to a proof of a corresponding property of $D(M)$.

To tie in the present work with **(2)** we will need the following remarks. Let $R = P \otimes_K P'$, and let S be the natural image in R of $Q \otimes_K P'$, where the $'$ denotes reciprocal ring. For an R-module W, Hochschild **(5)** defines $H^1(P, Q; W)$ to be $\mathrm{Ext}^1_{(R,S)}(P, W)$, P being considered naturally as an R-module. If $K = Q$, $H^1(P, Q; W) = H^1(P, W)$, the right-hand group being taken in the sense of cohomology of K-algebras **(1)**. If M and N are P-modules, $\mathrm{Hom}_K(M, N)$ is given the structure of an R-module, and it is proved that there exists a natural isomorphism

$$H^1(P, Q; \mathrm{Hom}_K(M, N)) = \mathrm{Ext}^1_{(P,Q)}(M, N)$$

which is readily seen to be a K-isomorphism **(5)**.

We define $D(P, Q) = \{x \in K | x \cdot H^1(P, Q; W) = 0 \text{ for all } R\text{-modules } W\}$. In other words, $D(P, Q) = D_{(R,S)}(P)$. As a consequence of the above isomorphism we have

LEMMA 4. *$D(P, Q) \subseteq D(M) \cap C(M)$. for any P-module M.*

We remark finally that it is natural to define

$$D^i(M) = \{x \in K | x \cdot \mathrm{Ext}^i(M, N) = 0 \text{ for all } P\text{-modules } N\},$$

and to define $C^i(M)$ and $D^i(P, Q)$ similarly $(i = 1, 2, \ldots,)$. Then the reduction theorem **(5)** gives $D^1(M) \subseteq D^2(M) \subseteq \ldots$, and similar inclusions for the others. Moreover, Lemmas 3 and 4 hold for arbitrary D^i, not just for $D = D^1$. The applications in this paper are restricted to the case $i = 1$.

Results equivalent to Lemmas 1-4 were established in **(3)**, but in a form not so convenient for our present purposes as the above.

2. Orders and principal modules. In this section, $\mathfrak{o}$ will denote an integral domain, and $\mathfrak{O}$ will denote an $\mathfrak{o}$-*order*, that is, an $\mathfrak{o}$-algebra which is regular as an $\mathfrak{o}$-module. Here an $\mathfrak{o}$-module is called *regular* if it is finitely generated and torsion free. It will be convenient to refer to an $\mathfrak{o}$-regular $\mathfrak{O}$-module as an $\mathfrak{O}$-*representation module*. We shall in particular determine the $\mathfrak{O}$-representation modules M such that $D(M) \neq 0$ or $C(M) \neq 0$, where

$$D(M) = D_{(\mathfrak{O}, \mathfrak{o})}(M) \quad \text{and} \quad C(M) = C_{(\mathfrak{O}, \mathfrak{o})}(M)$$

as defined in § 1.

First we introduce some notations useful here and in the later sections. If L is an integral domain containing $\mathfrak{o}$ as subdomain, we shall refer to the L-order

$$\mathfrak{O}_L = \mathfrak{O} \otimes_{\mathfrak{o}} L$$

as the *L-hull* of $\mathfrak{O}$. The *L-hull* of an $\mathfrak{O}$-module M is defined to be the $\mathfrak{O}_L$-module

$$M \otimes_{\mathfrak{O}} \mathfrak{O}_L = M \otimes_{\mathfrak{o}} L.$$

If k is the quotient field of $\mathfrak{o}$, k-hulls are referred to as *rational hulls*. Two $\mathfrak{O}$-modules M and N will be called *rationally equivalent* if their rational hulls are isomorphic. We shall also say that M is *rationally equivalent to an A-module V*, $A = \mathfrak{O}_k$, if the rational hull of M is isomorphic to V.

The L-hull M_L of an $\mathfrak{O}$-representation module M is an $\mathfrak{O}_L$-representation module, and, moreover, the natural homomorphisms $M \to M_L$ and

$$M \otimes_{\mathfrak{o}} \mathfrak{O} \to [M \otimes_{\mathfrak{o}} \mathfrak{O}]_L = M_L \otimes_L \mathfrak{O}_L$$

are $\mathfrak{O}$-monomorphisms. Hence the following lemma is an almost obvious consequence of Lemma 2.

LEMMA 5. *If L is a ring of quotients of $\mathfrak{o}$ and M is an $\mathfrak{O}$-representation module, then*

$$D_{(\mathfrak{O}_L,\, L)}(M_L) = L \cdot D_{(\mathfrak{O},\, \mathfrak{o})}(M).$$

Similarly

$$C_{(\mathfrak{O}_L,\, L)}(M_L) = L \cdot C_{(\mathfrak{O},\, \mathfrak{o})}(M).$$

An $\mathfrak{O}$-representation module M will be called a *principal $\mathfrak{O}$-module* if it is rationally equivalent to a direct sum of right ideal components of the rational hull A of $\mathfrak{O}$. On the other hand, M will be called *coprincipal* if it is rationally equivalent to a direct sum of A-module components of the A-module $\mathrm{Hom}_k(A, k)$.

THEOREM 1. *An $\mathfrak{O}$-representation module M is principal (coprincipal) if and only if $D(M) \neq 0$ ($C(M) \neq 0$).*

Proof. According to Lemma 5, $D(M) \neq 0$ is equivalent to $D_{(A,k)}(M_k) = k$, which in turn is equivalent by Lemma 1 to the (A, k)-projectiveness of M_k. But (A, k)-projectiveness coincides with A-projectiveness since k is a field, and it is well known that the A-projective modules are isomorphic with direct sums of right ideal components of A.

COROLLARY 1. *$D(M) \neq 0$ ($C(M) \neq 0$) for every $\mathfrak{O}$-representation module M if and only if the rational hull A of $\mathfrak{O}$ is semi-simple.*

Proof. Every A-representation module is the rational hull of some $\mathfrak{O}$-representation module. Hence by Theorem 1, $D(M) \neq 0$ for every $\mathfrak{O}$-representation module M if and only if every A-representation module is isomorphic with a direct sum of right ideal components of A. The latter condition is equivalent to the semi-simplicity of A.

The ideal $I(\mathfrak{O})$ defined in **(2)** coincides with the ideal $D(\mathfrak{O}, \mathfrak{o})$ as we see from the last part of § 1. The following theorem was proved more directly in **(2)**.

THEOREM 2. *A necessary and sufficient condition for $\mathfrak{O}$ to have separable rational hull is that $I(\mathfrak{O})$ be non-zero.*

Proof. By a theorem of Hochschild, $A = \mathfrak{O}_k$ is separable if and only if $H^1(A, W) = 0$ for all $A \otimes_k A'$-modules W. But $H^1(A, W) = H^1(A, k; W)$, so A is separable if and only if $1 \in D(A, k)$. Using Lemma 2 we readily obtain that $D(A, k) = k \cdot D(\mathfrak{O}, \mathfrak{o}) = k \cdot I(\mathfrak{O})$. Hence $1 \in D(A, k)$ if and only if $I(\mathfrak{O}) \neq 0$.

According to Lemma 4, $I(\mathfrak{O}) \subseteq D(M)$ for every $\mathfrak{O}$-module M. Hence it is a consequence of Theorem 2 that for separable A, $\bigcap D(M) \neq 0$, where the intersection extends over all $\mathfrak{O}$-modules M ($\mathfrak{o}$ regular or not). The result of **(4)** implies the existence of non-separable but semi-simple A such that for every A-representation module V, $\bigcap D(M) \neq 0$, where the intersection extends over all $\mathfrak{O}$-representation modules rationally equivalent to V. In fact, the Theorem of **(4)** implies the existence of such A for which every A-representation module has finite class number. It is of interest that $\bigcap D(M)$ may be zero when the intersection extends over the $\mathfrak{O}$-representation modules M rationally equivalent to a given right ideal component of A. For example, if $\mathfrak{O}$ is taken to be the Z-order of all matrices

$$X = \begin{pmatrix} x & y \\ & z \end{pmatrix}$$

with x, y, and z in the ring Z of rational integers, the $\mathfrak{O}$-representation module M_n corresponding to the matrix representation mapping X onto

$$\begin{pmatrix} x & ny \\ & z \end{pmatrix}$$

for fixed rational integer n has $D(M_n) = nZ$, as is readily seen using Lemma 2. Hence $\bigcap D(M_n) = 0$. Further, every M_n ($n = 1, 2, \ldots,$) is rationally equivalent to the same indecomposable right ideal component of the rational hull A of $\mathfrak{O}$. Of course A is not semi-simple.

The following additional remarks may be in order here. We noted at the end of § 1 that the ideal $I(\mathfrak{O}) = D(\mathfrak{O}, \mathfrak{o})$ is merely the first member of an ascending chain of ideals of $\mathfrak{o}$: $I(\mathfrak{O}) = I^1(\mathfrak{O}) \subseteq I^2(\mathfrak{O}) \subseteq \ldots$, $I^n(\mathfrak{O}) = D^n(\mathfrak{O}, \mathfrak{o})$. If $\mathfrak{o}$ satisfies the ascending chain condition, there is a first n such that $I^n(\mathfrak{O}) = I^{n+1}(\mathfrak{O}) = \ldots$, and it may be of interest to ask what is the

significance of this n for separable A. It follows from a result of **(3)** that $n = 1$ for a group ring $\mathfrak{O}$. Similar remarks apply to $D(M)$ and $C(M)$. It may also be of interest to look in the set T of $\mathfrak{O}$-representation modules rationally equivalent to a given right ideal component of A for those such that $D(M)$ is maximal for $M \in T$. When can we find $D(M) = \mathfrak{o}$, that is, M $(\mathfrak{O}, \mathfrak{o})$-projective? In this regard see Theorem 11 following.

3. The local case. In this and the next two sections we assume that $\mathfrak{o}$ is a local domain, that is, that $\mathfrak{o}$ is a principal ideal domain in which the non-units constitute the unique prime ideal $\mathfrak{p} = \pi\mathfrak{o}$. As always, $\mathfrak{O}$ denotes an $\mathfrak{o}$-order.

For an integer $s \geqslant 0$, $\mathfrak{o}^{(s)}$ will denote $\mathfrak{o}/\pi^s \cdot \mathfrak{o}$, and $\mathfrak{O}^{(s)}$ will denote the $\mathfrak{o}^{(s)}$-algebra $\mathfrak{O}/\pi^s \cdot \mathfrak{O}$. It is the main purpose of this and the next section to study relations between the representation theory of $\mathfrak{O}$, $\mathfrak{O}^{(s)}$, and the rational hull of $\mathfrak{O}$ The results are largely generalizations of results obtained by Maranda **(6; 7)** for the group case, and extensions of some results of Reiner **(8)** also arise.

The $\mathfrak{o}$-module $M/\pi^s \cdot M$ will be denoted by $M^{(s)}$, and can be considered as an $\mathfrak{o}^{(s)}$-module. If M is an $\mathfrak{O}$-module, so is $M^{(s)}$, and $M^{(s)}$ may be considered as an $\mathfrak{O}^{(s)}$-module. For $f \in \mathrm{Hom}\dagger\,(M, N)$, $f^{(s)}$ will denote[1] the natural image in $\mathrm{Hom}\dagger(M^{(s)}, N^{(s)})$; if f is an $\mathfrak{O}$-homomorphism, so is $f^{(s)}$. We shall say that $\mathfrak{O}$-modules M and N are *isomorphic modulo* $\mathfrak{p}^s$ if $M^{(s)}$ and $N^{(s)}$ are isomorphic as $\mathfrak{O}$-modules or, what is the same thing, as $\mathfrak{O}^{(s)}$-modules.

As in § 1, we may use the standard $(\mathfrak{O}, \mathfrak{o})$-projective resolution of an $\mathfrak{O}$-module M to compute $\mathrm{Ext}^1(M, N)$. Taking into account the natural $\mathfrak{O}$-isomorphisms

$$[M \otimes_{\mathfrak{o}} \mathfrak{O}]^{(s)} \simeq M^{(s)} \otimes_{\mathfrak{o}} \mathfrak{O} \simeq M^{(s)} \otimes_{\mathfrak{o}^{(s)}} \mathfrak{O}^{(s)},$$

we see that if

$$\ldots \xrightarrow{\chi_1} K_1 \otimes_{\mathfrak{o}} \mathfrak{O} \xrightarrow{\chi_0} M \otimes_{\mathfrak{o}} \mathfrak{O} \to 0$$

is the standard $(\mathfrak{O}, \mathfrak{o})$-projective resolution of M, then

$$\ldots \xrightarrow{\chi_1^{(s)}} [K_1 \otimes_{\mathfrak{o}} \mathfrak{O}]^{(s)} \xrightarrow{\chi_0^{(s)}} [M \otimes_{\mathfrak{o}} \mathfrak{O}]^{(s)} \to 0$$

may be identified with the standard $(\mathfrak{O}, \mathfrak{o})$-projective resolution of $M^{(s)}$ considered as an $\mathfrak{O}$-module, or with the standard $(\mathfrak{O}^{(s)}, \mathfrak{o}^{(s)})$-projective resolution of $M^{(s)}$ considered as an $\mathfrak{O}^{(s)}$-module. We shall denote by $X^{(s)}$ the left $\mathfrak{O}$-complex determined by this resolution, and by X the left $\mathfrak{O}$-complex determined by the standard $(\mathfrak{O}, \mathfrak{o})$-projective resolution of M. Then

[1] A dagger on the homomorphism (Hom†) indicates that the homomorphism is taken with respect to the domain $\mathfrak{o}$.

$$\mathrm{Ext}^1_{(\mathfrak{O},\,\mathfrak{o})}(M^{(s)}, N^{(s)})$$

is the 1-dimensional cohomology group of $\mathrm{Hom}^{\ddagger}(X^{(s)}, N^{(s)})$, and

$$\mathrm{Ext}^1_{(\mathfrak{O}^{(s)},\,\mathfrak{o}^{(s)})}(M^{(s)}, N^{(s)})$$

is the 1-dimensional cohomology group of

$$\mathrm{Hom}_{\mathfrak{O}^{(s)}}(X^{(s)}, N^{(s)}),$$

which is merely $\mathrm{Hom}^{\dagger}(X^{(s)}, N^{(s)})$ considered as an $\mathfrak{o}^{(s)}$-complex.[2] Thus

$$\mathrm{Ext}^1_{(\mathfrak{O}^{(s)},\,\mathfrak{o}^{(s)})}(M^{(s)}, N^{(s)})$$

is simply

$$\mathrm{Ext}^1_{(\mathfrak{O},\,\mathfrak{o})}(M^{(s)}, N^{(s)})$$

considered as an $\mathfrak{o}^{(s)}$-module. It follows that

$$D_{(\mathfrak{O}^{(s)},\,\mathfrak{o}^{(s)})}(M^{(s)}) = [D_{(\mathfrak{O},\,\mathfrak{o})}(M^{(s)}) + \mathfrak{p}^{(s)}]/\mathfrak{p}^{(s)},$$

a fact that is also readily seen from Lemma 2.

We now prove the following generalization of Maranda's Theorem 2 of **(6)**.

THEOREM 3. *Let M and N be $\mathfrak{O}$-representation modules, and assume that*

$$\pi^s \cdot \mathrm{Ext}^1_{(\mathfrak{O},\,\mathfrak{o})}(M, N) = 0.$$

Then M and N are isomorphic if and only if they are isomorphic modulo $\mathfrak{p}^{s+1}$.

Proof. An $\mathfrak{O}$-isomorphism $M^{(s+1)} \simeq N^{(s+1)}$ is induced by an $\mathfrak{o}$-isomorphism $\beta : M \simeq N$, for M and N have free $\mathfrak{o}$-module bases since $\mathfrak{o}$ is a principal ideal domain. Then for $u \in M$, $\omega \in \mathfrak{O}$, $\beta(u\omega) - \beta(u)\omega \in \pi^{s+1} \cdot N$. Let

$$^*: \mathrm{Hom}_{\mathfrak{o}}(M, N) \simeq \mathrm{Hom}_{\mathfrak{O}}(M \otimes_{\mathfrak{o}} \mathfrak{O}, N)$$

be the natural isomorphism, then this identity means that $\chi_0\beta^* \equiv 0 \pmod{(\pi^{s+1})}$. Hence there exists

$$f \in \mathrm{Hom}_{\mathfrak{o}}(M \otimes_{\mathfrak{o}} \mathfrak{O}, N)$$

such that

$$\chi_0\beta^* = \pi^{s+1} \cdot f.$$

Since χ_0 and β^* are $\mathfrak{O}$-homomorphisms, so is f. And

$$0 = \chi_1\chi_0\beta^* = \pi^{s+1}\chi_1 f,$$

[2] A double dagger on the homomorphism ($\mathrm{Hom}^{\ddagger}$) indicates that the homomorphism is taken with respect to the order $\mathfrak{O}$.

so $\chi_1 f = 0$ and f is a 1-cocycle. The assumption of the theorem therefore implies that $\pi^s f$ is a coboundary, and hence that there exists $g \in \mathrm{Hom}\dagger\,(M, N)$ such that $\pi^s \cdot f = \chi_0 g^*$. Let $\alpha = \beta - \pi^s \cdot g$, then $\chi_0 \alpha^* = \chi_0 \beta^* - \pi \chi_0 g^* = \pi^{s+1} \cdot f - \pi(\pi^s f) = 0$, which implies that α is an element of $\mathrm{Hom}\dagger\,(M, N)$. Since β induces an isomorphism $M^{(s+1)} \simeq N^{(s+1)}$, $\det \beta \notin \mathfrak{p}$. But $\det \alpha \equiv \det \beta \pmod{\mathfrak{p}}$, so $\det \alpha \notin \mathfrak{p}$. Hence $\det \alpha$ is a unit in $\mathfrak{o}$ and $\alpha : M \simeq N$.

Since the converse is immediate, the proof of Theorem 3 is complete.

We now define the *depth* (*codepth*) of an $\mathfrak{O}$-module M to be s if $D(M) = \mathfrak{p}^s$ ($C(U) = \mathfrak{p}^s$) and ∞ if $D(M) = 0$ ($C(M) = 0$). Thus by Theorem 1, the principal $\mathfrak{O}$-modules are the $\mathfrak{O}$-representation modules of finite depth (codepth).

An immediate consequence of this definition of depth and Theorem 3 is

COROLLARY 1. *A principal* (*coprincipal*) $\mathfrak{O}$*-module of depth* s (*codepth* s) *is isomorphic with an* $\mathfrak{O}$*-representation module* N *if and only if* M *and* N *are isomorphic modulo* $\mathfrak{p}^{s+1}$.

Simple examples of the sort given at the end of § 2 show that the number of non-isomorphic $\mathfrak{O}$-representation modules rationally equivalent to a given $\mathfrak{O}_k$-representation module V may be infinite, even if V is an indecomposable right ideal component of $\mathfrak{O}_k$ and $\mathfrak{o}$ has finite residue class rings. But we do have

COROLLARY 2. *If* $\mathfrak{o}^{(s+1)}$ *is finite, the number of non-isomorphic* $\mathfrak{O}$*-representation modules of depth* (*codepth*) s *and given rank is finite.*

Proof. Corollary 1 implies that the isomorphism class of M is determined by the isomorphism class of $M^{(s+1)}$. But $\mathfrak{O}^{(s+1)}$ and $M^{(s+1)}$ have only finitely many elements as finitely generated modules over the finite ring $\mathfrak{o}^{(s+1)}$.

If the rational hull of $\mathfrak{O}$ is separable, $I(\mathfrak{O}) = D(\mathfrak{O}, \mathfrak{o})$ is non-zero by Theorem 2, hence $I(\mathfrak{O}) = \mathfrak{p}^t$. We call t the *depth* of $\mathfrak{O}$. By Lemma 4, $I(\mathfrak{O}) \subseteq D(M)$ for every $\mathfrak{O}$-module M, hence $0 \leqslant \mathrm{depth}\ M \leqslant t$ for every $\mathfrak{O}$-module M. Hence in this case Corollary 2 implies

COROLLARY 3. *If* $\mathfrak{O}$ *has separable rational hull and* $\mathfrak{o}$ *has finite residue class rings, then the number of non-isomorphic* $\mathfrak{O}$*-representation modules of given rank is finite.*

We now show that depth is preserved under the transition to the complete case. Let k_* denote the completion of the quotient field k of $\mathfrak{o}$ with respect to the valuation determined by $\mathfrak{p}$. Let $\mathfrak{o}_*$ be the valuation ring of k_*, and let $\mathfrak{p}_* = \pi \mathfrak{o}_*$ be the valuation ideal. We denote by $\mathfrak{O}_*$ and M_* the $\mathfrak{o}_*$- hulls of $\mathfrak{O}$ and M respectively.

THEOREM 4. *For an* $\mathfrak{O}$*-representation module* M,

$$D_{(\mathfrak{O}, \mathfrak{o})}(M) = D_{(\mathfrak{O}_*, \mathfrak{o}_*)}(M_*) \cap \mathfrak{o}_*$$

and

$$C_{(\mathfrak{O},\mathfrak{o})}(M) = C_{(\mathfrak{O}_*,\mathfrak{o}_*)}(M_*) \cap \mathfrak{o}_*.$$

Proof. We use Lemma 2, according to which $x \in \mathfrak{o}$ belongs to $D(M)$ if and only if there exists an $\mathfrak{O}_k$-homomorphism

$$\beta : M_k \to [M \otimes_{\mathfrak{o}} \mathfrak{O}]_k$$

such that

(i) $\beta\tau_k = x \cdot I$, where

$$\tau_k : [M \otimes_{\mathfrak{o}} \mathfrak{O}]_k \to M_k$$

is induced by the natural homomorphism

$$\tau : M \otimes_{\mathfrak{o}} \mathfrak{O} \to M,$$

and I is the identity map of M_k, and

(ii) $\beta(M) \subseteq M \otimes_{\mathfrak{o}} \mathfrak{O}$, where M and $M \otimes_{\mathfrak{o}} \mathfrak{O}$ are identified with their natural images in M_k and $[M \otimes_{\mathfrak{o}} \mathfrak{O}]_k$ respectively.

Since $\mathfrak{o}$ is a principal ideal domain, there exist free $\mathfrak{o}$-module bases $u_1, \ldots, u_m$ and $v_1, \ldots, v_n$ of M and $M \otimes_{\mathfrak{o}} \mathfrak{O}$ respectively. If we write $\beta(u_i) = \sum a_{ij} v_j$, then for given $x \in \mathfrak{o}$, (i) may be expressed as a system of linear equations in the unknowns a_{ij}, with coefficients in $\mathfrak{o}$. The condition that x be in $D(M_*)$ means that the system has a solution in $\mathfrak{o}_*$. But a solution exists in $\mathfrak{o}_*$ if and only if one exists in $\mathfrak{o}$, that is, if and only if $x \in D(M)$, proving Theorem 4.

According to the definition of depth given above, Theorem 4 can be restated as

COROLLARY 1. *The depth of an $\mathfrak{O}$-representation module M is equal to the depth of its $\mathfrak{o}^*$-hull M^*.*

An important consequence for our purposes is the following extension of Corollary 1 to Theorem 1 of Maranda's paper **(7)**.

COROLLARY 2. *A principal (coprincipal) $\mathfrak{O}$-module M is isomorphic with an $\mathfrak{O}$-representation module N if and only if M_* and N_* are isomorphic.*

Proof. Suppose M has depth s, then $D(M_*) = \pi^s \mathfrak{o}_*$ by Corollary 1. Now $\mathfrak{o}^{(s+1)} \simeq \mathfrak{o}_*^{(s+1)}$, and, as $\mathfrak{o}^{(s+1)}$-algebras, $\mathfrak{O}^{(s+1)} \simeq \mathfrak{O}_*^{(s+1)}$. Further, as $\mathfrak{O}^{(s+1)}$-modules, $M^{(s+1)} \simeq M_*^{(s+1)}$. The result now follows by Corollary 1 to Theorem 3.

We remark that a similar application of Lemma 2 proves that $I(\mathfrak{O}) = I(\mathfrak{O}_*) \cap \mathfrak{o}$, and hence that the depth of $\mathfrak{O}$ is equal to that of $\mathfrak{O}_*$.

4. The complete case. We retain the notation of § 3, and assume in addition that k is *complete*, that is, that $k = k_*$.

We need the following remark, which depends only on the fact that $\mathfrak{o}$ is a principal ideal domain.

LEMMA 6. *Given $\mathfrak{O}$-representation modules M and N, and $s \geqslant 0$, every $\mathfrak{O}$-homomorphism*

$$[M \otimes_{\mathfrak{o}} \mathfrak{O}]^{(s)} \to N^{(s)}$$

is induced by an $\mathfrak{O}$-homomorphism $M \otimes_{\mathfrak{o}} \mathfrak{O} \to N$.

Proof. Denote by * the natural isomorphism

$$\mathrm{Hom}_{\mathfrak{o}}(U, V) \cong \mathrm{Hom}_{\mathfrak{O}}(U \otimes_{\mathfrak{o}} \mathfrak{O}, V)$$

for any two $\mathfrak{O}$-modules U and V. If

$$g \in \mathrm{Hom}_{\mathfrak{O}}([M \otimes_{\mathfrak{o}} \mathfrak{O}]^{(s)}, N^{(s)}),$$

then $g = h^*$ for some $h \in \mathrm{Hom}\dagger\,(M^{(s)}, N^{(s)})$. Since $\mathfrak{o}$ is a principal ideal domain, there exists $f \in \mathrm{Hom}\dagger\,(M, N)$ inducing h. But then

$$f^* \in \mathrm{Hom}_{\mathfrak{O}}(M \otimes_{\mathfrak{o}} \mathfrak{O}, N)$$

induces $h^* = g$. Here we have used the natural identification of

$$M^{(s)} \otimes_{\mathfrak{o}} \mathfrak{O} \quad \text{with} \quad [M \otimes_{\mathfrak{o}} \mathfrak{O}]^{(s)}.$$

A homological extension of a result of Reiner **(8)** is the following.

THEOREM 5. *If M and N are $\mathfrak{O}$-representation modules, then*

$$\pi^s \cdot \mathrm{Ext}^1\,(M^{(s+1)}, N^{(s+1)}) = 0$$

implies $\pi^s \cdot \mathrm{Ext}^1(M, N) = 0$.

Proof. Suppose that $\pi^s \cdot \mathrm{Ext}^1(M^{(s+1)}, N^{(s+1)}) = 0$, and let X be the left $\mathfrak{O}$-complex determined by the standard $(\mathfrak{O}, \mathfrak{o})$-projective resolution of M. If $f : K_1 \otimes_{\mathfrak{o}} \mathfrak{O} \to N$ is a 1-cocycle for $\mathrm{Hom}\ddagger(X, N)$, then $f^{(s+1)}$ is a 1-cocycle for $\mathrm{Hom}\ddagger(X^{(s+1)}, N^{(s+1)})$. (The notations X and $X^{(s+1)}$ refer to the left $\mathfrak{O}$-complexes obtained from the standard $(\mathfrak{O}, \mathfrak{o})$-projective resolutions of M and $M^{(s+1)}$ respectively, cf. the third paragraph of § 3.) Hence $\pi^s \cdot f^{(s+1)}$ is a coboundary, which means, using Lemma 6, that there exists an $\mathfrak{O}$-homomorphism $g_0 : M \otimes_{\mathfrak{o}} \mathfrak{O} \to N$ such that

$$\pi^s \cdot f \equiv \chi_0 g_0 \pmod{(\pi^{s+1})},$$

that is, there exists an $\mathfrak{o}$-homomorphism $f_1 : K_1 \otimes_{\mathfrak{o}} \mathfrak{O} \to N$ such that

$$\pi^s \cdot f = \chi_0 g_0 + \pi^{s+1} \cdot f_1.$$

Since f and $\chi_0 g_0$ are $\mathfrak{O}$-homomorphisms, so is f_1. Since f is a cocycle,

$$\pi^{s+1} \cdot \chi_1 f_1 = \pi^s \cdot \chi_1 f - \chi_1 \chi_0 g_0 = 0,$$

so f_1 is a cocycle. Hence, repetition of the above produces an $\mathfrak{O}$-homomorphism $g_1 : M \otimes_{\mathfrak{o}} \mathfrak{O} \to N$ and an $\mathfrak{o}$-homomorphism $f_2 : K_1 \otimes_{\mathfrak{o}} \mathfrak{O} \to N$ such that $\pi^s \cdot f_1 = \chi_0 g_1 + \pi^{s+1} \cdot f_2$. Then

$$\pi^s \cdot f = \chi_0(g_0 + \pi \cdot g_1) + \pi^{s+2} \cdot f,$$

and again we see that f_2 is a cocycle. Continuing in this way we obtain $\mathfrak{O}$-homomorphisms

$$g_i : K_1 \otimes_{\mathfrak{o}} \mathfrak{O} \to N (i = 0, 1, \ldots,)$$

such that

$$\pi^s \cdot f \equiv \chi_0(g_0 + \pi \cdot g_1 + \ldots + \pi^i \cdot g_i) \pmod{\mathfrak{p}^{s+i+1}}.$$

Since k is complete, we may define $g = g_0 + \pi \cdot g_1 + \ldots + \pi^i \cdot g_i + \ldots$, and conclude that $\pi^s \cdot f = \chi_0 g$ is a coboundary. Hence $\pi^s \cdot \mathrm{Ext}^1(M, N) = 0$, proving Theorem 5.

COROLLARY 1. *An $\mathfrak{O}$-representation module M has depth (codepth) s if and only if $M^{(s+1)}$ has depth (codepth) s (as an $\mathfrak{O}$-module).*

Proof. By Theorem 5, if $M^{(s+1)}$ has depth s, M has depth $\leqslant s$. But it follows at once from Lemma 2 and the existence of the natural isomorphism

$$[M \otimes_{\mathfrak{o}} \mathfrak{O}]^{(s)} = M^{(s)} \otimes_{\mathfrak{o}} \mathfrak{O}$$

that the depth of M is $\leqslant$ the depth of $M^{(t)}$ for any t.

Since by Lemma 1 the $\mathfrak{O}$-modules of depth O (codepth O) are precisely the $(\mathfrak{O}, \mathfrak{o})$-projective (injective) ones, the case $s = 0$ of Corollary 1 gives

COROLLARY 2. *An $\mathfrak{O}$-representation module M is $(\mathfrak{O}, \mathfrak{o})$-projective (injective) if and only if $M/\pi \cdot M$ is $(\mathfrak{O}, \mathfrak{o})$-projective (injective).*

This is a slight improvement of a result of Reiner **(8)** since the "only if" part does not require special hypotheses. Note the $(\mathfrak{O}, \mathfrak{o})$-projectiveness and $(\mathfrak{O}/\pi \cdot \mathfrak{O}, \mathfrak{o}/\pi \cdot \mathfrak{o})$-projectiveness coincide for an $\mathfrak{O}/\pi \cdot \mathfrak{O}$-module.

We observe, without including the details, that essentially the same argument used to prove Theorem 5 and Corollary 1 proves

THEOREM 6. *$\mathfrak{O}$ has depth t if and only if $D(\mathfrak{O}^{(t+1)}, \mathfrak{o}) = \mathfrak{p}^t(\mathfrak{O}^{(t+1)}$ being considered as an $\mathfrak{o}$-algebra).*

The case $t = O$, combined with Hochschild's characterization of separable algebras gives the

COROLLARY: *$\mathfrak{O}$ has depth O if and only if $\mathfrak{O}/\pi \cdot \mathfrak{O}$ is a separable $\mathfrak{o}/\pi \cdot \mathfrak{o}$-algebra.*

For application in § 5 we need

THEOREM 7 (Brauer). *If H is an $(\mathfrak{O}, \mathfrak{o})$-projective (injective) $\mathfrak{O}$-representation module, and if U is an $\mathfrak{O}$-module direct summand of $H/\pi \cdot H$, then there exists an $\mathfrak{O}$-module direct summand M of H such that $M/\pi \cdot M \cong U$.*

We will derive this theorem here as a corollary to an extension of a variant of Maranda's Theorem 3 of **(6)**.

If M is a primitive $\mathfrak{o}$-submodule of an $\mathfrak{O}$-representation module H (that is, an $\mathfrak{o}$-module direct summand), we may identify $M^{(s)} = M/\pi \cdot M$ with the $\mathfrak{o}$-submodule $(M + \pi^s \cdot H)/\pi^s \cdot H$ of $H^{(s)}$, and then we may identify $[H/M]^{(s)}$ with $H^{(s)}/M^{(s)}$. Then $M^{(s)}$ is an $\mathfrak{O}$-submodule of $H^{(s)}$ if and only if $M\mathfrak{O} \subseteq M + \pi^s \cdot H$, and every $\mathfrak{o}$-primitive $\mathfrak{O}$-submodule of $H^{(s)}$ is obtained in this way from a primitive $\mathfrak{o}$-submodule of H.

THEOREM 8. *Let M be a primitive $\mathfrak{o}$-submodule of an $\mathfrak{O}$-representation module H, such that $M\mathfrak{O} \subseteq M + \pi^{s+1} \cdot H$ and $M^{(s+1)}$ has depth s as an $\mathfrak{O}$-module. Then there exists an $\mathfrak{O}$-submodule M^* of H of depth s, and primitive as an $\mathfrak{o}$-submodule, such that $M^{*(s+1)} = M^{(s+1)}$.*

Proof. We construct a sequence $M_0, M_1, \ldots, M_t, \ldots$, of primitive $\mathfrak{o}$-submodules of H such that $M_t\mathfrak{O} \subseteq M_t + \pi^{s_t} \cdot H$, $s_0 = s + 1$, $s_{t+1} = s_t + 1$, and $M_{t+1}{}^{(s+1)} = M_t{}^{(s+1)}$. The existence of an $\mathfrak{o}$-primitive $\mathfrak{O}$-submodule M^* of H with $M^{*(s+1)} = M^{(s+1)}$ then follows by the completeness of k. Since $M^{(s+1)}$ has depth s, Corollary 1 to Theorem 5 implies that M^* also has depth s.

The M_t are constructed inductively. Let $M_0 = M$, and assume that M_t has been constructed. Since M_t is primitive, there exists an $\mathfrak{o}$-submodule N of H such that $H = M_t \oplus N$. Then

$$M_t\mathfrak{O} \subseteq M_t + \pi^{s_t} \cdot H = M_t \oplus \pi^{s_t} \cdot N.$$

Thus, for $u \in M_t$ and $\omega \in \mathfrak{O}$, there exist unique elements $\sigma(u, \omega) \in M_t$ and $\tau(u, \omega) \in N$ such that

$$u\omega = \sigma(u, \omega) + \pi^{s_t} \cdot \tau(u, \omega).$$

We denote by T the $\mathfrak{O} \otimes_{\mathfrak{o}} \mathfrak{O}'$-module

$$\mathrm{Hom}_{\mathfrak{o}}(M_t^{(s+1)}, [H/M_t]^{(s+1)}),$$

and by τ^+ the element of $\mathrm{Hom}^\dagger(\mathfrak{O}, T)$ such that $\tau^+(\omega)\{\bar{u}\}$ is the residue class modulo $\pi^{s+1} \cdot [H/M_t]$ of $M_t + \tau(u, \omega) \in H/M_t$, where $\bar{u}$ is the residue class modulo $\pi^{s+1} \cdot M_t$ of $u \in M_t$. From the associative law $u(\xi\eta) = (u\xi)\eta$ we get the identity

$$\tau(u, \xi\eta) = \tau(\sigma(u, \xi), \eta) + \tau(u, \xi)\eta,$$

which means that τ^+ is a 1-cocycle for the complex with homogeneous components $C^n(\mathfrak{O}, \mathfrak{o}; T)$ described in **(6, § 3)**. Since the 1-dimensional cohomology group of this complex is $\mathrm{Ext}^1(M_t{}^{(s+1)}, [H/M_t]^{(s+1)})$, and since $M_t{}^{(s+1)} = M^{(s+1)}$ has depth s, it follows that $\pi^s \cdot \tau^+$ is a coboundary. Hence there exists $g \in \mathrm{Hom}_{\mathfrak{o}}(H, N)$ such that for $u \in M_t$, $\omega \in \mathfrak{O}$,

$$\tau(u, \omega) = g(u\omega) - g(u)\omega + \pi^{s+1} \cdot \mu(u, \omega),$$

with $\mu(u, \omega) \in H$. Let $M_{t+1} = \{u + \pi^{s_t - s} \cdot g(u) | u \in M_t\}$, then M_{t+1} is a

primitive $\mathfrak{o}$-submodule of H since $H = M_{t+1} \oplus N$. Since $2s_t - s \geqslant s_t + 1 = s_{t+1}$, we have for $\omega \in \mathfrak{O}$ and $u \in M_t$ that

$$\begin{aligned}[u + \pi^{s_t - s} \cdot g(u)]\omega &= u\omega + \pi^{s_t - s} g(u)\omega \\ &= \sigma(u, \omega) + \pi^{s_t} \cdot \tau(u, \omega) + \pi^{s_t - s}\{g(u\omega) - \pi^{s} \cdot \tau(u, \omega) \\ &\qquad + \pi^{s+1} \cdot \mu(u, \omega) \\ &= \sigma(u, \omega) + \pi^{s_t - s} \cdot g(\sigma(u, \omega)) + \pi^{2s_t - s} \cdot g(\tau(u, \omega)) \\ &\qquad + \pi^{s_t + 1} \mu(u, \omega) \in M_{t+1} + \pi^{s_t + 1} H.\end{aligned}$$

Hence $M_{t+1}\mathfrak{O} \subseteq M_{t+1} + \pi^{s_t + 1} \cdot H$.

Now we define an $\mathfrak{o}$-module automorphism ϕ of H by mapping $u \in M_t$ onto $u + \pi^{s_t - s} g(u)$, and $v \in N$ onto v, so that in particular $\phi(M_t) = M_{t+1}$. For $u \in M_t$ and $\omega \in \mathfrak{O}$.

$$\begin{aligned}\phi(u\omega) = \phi(\sigma(u, \omega) + \pi^{s_t} \cdot \tau(u, \omega)) &= \sigma(u, \omega) + \pi^{s_t - s} g(\sigma(u, \omega)) + \pi^{s_t} \cdot \tau(u, \omega) \\ &\equiv \sigma(u, \omega) + \pi^{s_t - s} \cdot g(\sigma(u, \omega)) \equiv \phi(u)\omega \pmod{(\pi^{s+1})}.\end{aligned}$$

We may conclude that $M_{t+1}{}^{(s+1)} \simeq M_t{}^{(s+1)}$, which means that the inductive construction of the M_t is complete.

We can deduce Theorem 7 from Theorem 8 and Corollary 2 to Theorem 5 as follows: Since H is $(\mathfrak{O}, \mathfrak{o})$-projective, so is $H/\pi \cdot H$ by Corollary 2 to Theorem 5, hence so is the $\mathfrak{O}$-module direct summand U. Theorem 8 (with $s = 0$) therefore implies the existence of an $(\mathfrak{O}, \mathfrak{o})$-projective $\mathfrak{O}$-submodule M such that $M/\pi M \simeq U$.

Another application of Theorem 8 is the following

COROLLARY. *Let U be an $\mathfrak{O}^{(s+1)}$-module, that is, an $\mathfrak{O}$-module such that $\pi^{s+1} \cdot U = 0$. If U has depth (codepth) s as an $\mathfrak{O}$-module, and is finitely generated and projective as an $\mathfrak{o}^{(s+1)}$-module, there exists an $\mathfrak{O}$-representation module M^* of depth (codepth) s such that $M^{*(s+1)} \simeq U$.*

Proof. Since U is a projective and finitely generated $\mathfrak{o}^{(s+1)}$-module, it is an $\mathfrak{o}^{(s+1)}$-module direct summand of a finitely generated free $\mathfrak{o}^{(s+1)}$-module V. Now there exists a regular $\mathfrak{o}$-module N such that $N^{(s+1)} \simeq V$. Moreover, there exists an $\mathfrak{O}$-isomorphism $\mathrm{Hom}\dagger(\mathfrak{O}, V) \simeq [\mathrm{Hom}(\mathfrak{O}, N)]^{(s+1)}$, and an $\mathfrak{O}$-monomorphism $U \to \mathrm{Hom}\dagger[\mathfrak{O}, V)$, namely, the composite $U \to \mathrm{Hom}\dagger(\mathfrak{O}, U) \to \mathrm{Hom}\dagger(\mathfrak{O}, V)$. It follows that there exists a primitive $\mathfrak{o}$-submodule M of $H = \mathrm{Hom}\dagger(\mathfrak{O}, N)$ such that $M\mathfrak{O} \subseteq M + \pi^{s+1}H$ and $M^{(s+1)} \simeq U$. The existence of M^* now follows from Theorem 8.

5. Projective modules in the complete case. We assume, as in the preceding section, that the quotient field k of $\mathfrak{o}$ is complete. Applying Theorems 3 and 7 we obtain

THEOREM 9 (Brauer). *Up to isomorphism and order of summands, every $(\mathfrak{O}, \mathfrak{o})$-projective $\mathfrak{O}$-representation module has a unique decomposition into a direct sum of indecomposable $\mathfrak{O}$-modules. If $\mathfrak{O} = \sum \oplus \mathfrak{O}_\alpha$, where the $\mathfrak{O}_\alpha$ are*

indecomposable right ideals, then $\mathfrak{O}/\pi\mathfrak{O} = \sum \oplus \mathfrak{O}_\alpha/\pi\mathfrak{O}_\alpha$ *is a decomposition of the* $\mathfrak{o}/\pi\mathfrak{o}$*-algebra* $\mathfrak{O}/\pi\mathfrak{O}$ *into indecomposable right ideals, and any indecomposable* $(\mathfrak{O}, \mathfrak{o})$*-projective* $\mathfrak{O}$*-representation module is isomorphic with one of the* $\mathfrak{O}_\alpha$.

Proof. Since $\mathfrak{O}/\pi\mathfrak{O}$ is a finite dimensional algebra over the field $\mathfrak{o}/\pi\mathfrak{o}$, $\mathfrak{O}/\pi\mathfrak{O} = \sum \oplus \bar{\mathfrak{O}}_\alpha$ with the $\bar{\mathfrak{O}}_\alpha$ indecomposable right ideals unique up to order and isomorphism. By Theorem 7, there exist right ideals $\mathfrak{O}_\alpha$ of $\mathfrak{O}$ such that $\mathfrak{O} = \sum \oplus \mathfrak{O}_\alpha$ and $\mathfrak{O}_\alpha/\pi\mathfrak{O}_\alpha \approx \bar{\mathfrak{O}}_\alpha$. Since the $\bar{\mathfrak{O}}_\alpha$ are indecomposable, Theorem 7 implies that the $\mathfrak{O}_\alpha$ are too.

If M is an $(\mathfrak{O}, \mathfrak{o})$-projective $\mathfrak{O}$-module, so is $M/\pi M$ by Corollary 2 to Theorem 5, and hence $M/\pi M$ is $(\mathfrak{O}/\pi\mathfrak{O}, \mathfrak{o}/\pi\mathfrak{o})$-projective. As is well known, this implies that $M/\pi M = \sum \oplus \bar{M}_\beta$, where each $\bar{M}_\beta$ is isomorphic to some $\mathfrak{O}_\alpha$. Hence by Theorem 7, $M = \sum \oplus M_\beta$, where each M_β is isomorphic to some $\mathfrak{O}_\alpha$.

Suppose that $M = \sum \oplus N_\gamma$, with each N_γ indecomposable. Then $N_\gamma/\pi N_\gamma$ is indecomposable by Theorem 7 and $M/\pi M = \sum \oplus N_\gamma/\pi N_\gamma$. Hence by the Krull-Schmidt theorem, the $\bar{M}_\beta$ and $N_\gamma/\pi N_\gamma$ are equal in number and isomorphic in pairs. Corollary 1 to Theorem 3 (with $s = 0$) implies therefore that the M_β and N_γ are isomorphic in pairs.

There is a similar result for $(\mathfrak{O}, \mathfrak{o})$-injective $\mathfrak{O}$-representation modules, which may be proved similarly.

We now generalize Maranda's Theorem 4 of **(7)**. It will be convenient to begin with two lemmas, the second of which is a special case of our thorem.

LEMMA 7. *If* $\mathfrak{O}$ *has depth O, and the* $\mathfrak{O}$*-representation module M has irreducible rational hull, then* $M/\pi M$ *is an irreducible* $\mathfrak{O}/\pi\mathfrak{O}$*-module.*

Proof. If $\mathfrak{O}$ has depth O, every $\mathfrak{O}$-module is $(\mathfrak{O}, \mathfrak{o})$-projective, and by the Corollary to Theorem 6, $\mathfrak{O}/\pi\mathfrak{O}$ is a separable $\mathfrak{o}/\pi\mathfrak{o}$-algebra. Hence $M/\pi M$ is fully reducible, and Theorem 7 implies that it is irreducible.

LEMMA 8. *If* $\mathfrak{O}$ *has depth* O, *two* $\mathfrak{O}$*-representation modules M and N with irreducible rational hulls are isomorphic if and only if their rational hulls are isomorphic.*

Proof. If M and N have isomorphic rational hulls, we may assume that $M \subseteq N$. By Lemma 7, $N/\pi N$ is irreducible, hence $M/\pi M \approx M + \pi N/\pi N = N/\pi N$. Corollary 1 to Theorem 3 implies therefore that $M \approx N$. The converse is immediate.

We let R denote the radical of the rational hull A of $\mathfrak{O}$. Then $\mathfrak{O}/\mathfrak{R}$ is an $\mathfrak{o}$-order with rational hull isomorphic to A/R, where $\mathfrak{R} = \mathfrak{O} \cap R$.

THEOREM 10. *If* $\mathfrak{O}/\mathfrak{R}$ *has depth O, then two* $(\mathfrak{O}, \mathfrak{o})$*-projective* $\mathfrak{O}$*-representation modules are isomorphic if and only if their rational hulls are isomorphic.*

Proof. Only the "if" part requires proof, and by Theorem 9 we have only to consider indecomposable $\mathfrak{O}$-representation modules.

Let M be an indecomposable $(\mathfrak{O}, \mathfrak{o})$-projective $\mathfrak{O}$-representation module, and let $V = M_k$. Then $V = V_1 \oplus \ldots \oplus V_t$, where the V_i may be taken to be indecomposable right ideal components of A according to Theorem 1. Let

$$W_i = X_i + \sum_{j \neq i} V_j,$$

where X_i is the unique maximal A-submodule of V_i. Then $V/W_i \simeq V_i/X_i$, the irreducible A-submodule determining the isomorphism class of V_i, which we shall denote by F_i. We show now that $F_i \simeq F$ $(i = 1, 2, \ldots, t)$, $F = F_1$.

We note first that $\mathfrak{F}_i = M/M \cap W_i$ is an $\mathfrak{O}$-representation module with rational hull isomorphic to F_i. Since $\mathfrak{F}_i$ can be considered as an $\mathfrak{O}/\mathfrak{R}$-module, Lemma 7 implies that $\mathfrak{F}_i/\pi\mathfrak{F}_i$ is an irreducible $\mathfrak{O}/\pi\mathfrak{O}$-module. Theorem 7 implies that $M/\pi M$ is an indecomposable $\mathfrak{O}/\pi\mathfrak{O}$-module, hence, since $\mathfrak{F}_i/\pi\mathfrak{F}_i$ is isomorphic with a quotient module of $M/\pi M$, it follows that $\mathfrak{F}_i/\pi\mathfrak{F}_i$ is uniquely determined by $M/\pi M$. That is, $\mathfrak{F}_i/\pi\mathfrak{F}_i \simeq \mathfrak{F}/\pi\mathfrak{F}$ $(i = 1, 2, \ldots, t)$, where $\mathfrak{F} = \mathfrak{F}_1$. Hence $\mathfrak{F}_i \simeq \mathfrak{F}$ by Corollary 1 to Theorem 3, which certainly implies $F_i \simeq F$.

Now let N be a second indecomposable $(\mathfrak{O}, \mathfrak{o})$-projective $\mathfrak{O}$-representation module such that $N_k \simeq V$, and let $\mathfrak{G}$ correspond to N as $\mathfrak{F}$ does to M. Then we must have $\mathfrak{G}_k \simeq F$, which implies $\mathfrak{G} \simeq \mathfrak{F}$ by Lemma 8. Hence $\mathfrak{G}/\pi\mathfrak{G} \simeq \mathfrak{F}/\pi\mathfrak{F}$, which implies $N/\pi N \simeq M/\pi M$. Hence $M \simeq N$ by Corollary 1 to Theorem 3.

An immediate consequence of the above proof is the following.

COROLLARY. *If $\mathfrak{O}/\mathfrak{R}$ has depth 0, then the rational hull of an indecomposable $\mathfrak{O}$-representation module M is isomorphic with a direct sum of isomorphic indecomopsable right ideal components of A.*

It must be remarked that the completeness of $\mathfrak{o}$ is inessential for Theorem 10 and its Corollary, for, by Corollary 1 to Theorem 4, and the remark at the end of § 3, the hypotheses survive transition from the local to the complete case, and by Corollary 2 to Theorem 4, if the conclusion holds relative to the completion of a local domain $\mathfrak{o}$, it holds relative to $\mathfrak{o}$.

6. The Dedekind case. In this final section we assume that $\mathfrak{o}$ is a Dedekind domain, and denote by $\mathfrak{o}_\mathfrak{p}$ the ring of quotients of $\mathfrak{o}$ with respect to the complement of the prime ideal $\mathfrak{p}$ of $\mathfrak{o}$, that is, the ring of $\mathfrak{p}$-integers in the quotient field k of $\mathfrak{o}$. By $\mathfrak{O}_\mathfrak{p}$ we denote the $\mathfrak{o}_\mathfrak{p}$-hull of the $\mathfrak{o}$-order $\mathfrak{O}$, and by $M_\mathfrak{p}$ the $\mathfrak{o}_\mathfrak{p}$-hull of an $\mathfrak{o}$-module M. A subscript $*$ refers to the $\mathfrak{p}$-adic completion as at the end of § 3.

According to Theorems 1 and 4, we have for any $\mathfrak{O}$-representation module M that

$$\mathfrak{o}_\mathfrak{p} \cdot D_{(\mathfrak{O}, \mathfrak{o})}(M) = D_{(\mathfrak{O}_\mathfrak{p}, \mathfrak{o}_\mathfrak{p})}(M_\mathfrak{p}) = D_{(\mathfrak{O}_{\mathfrak{p}*}, \mathfrak{o}_{\mathfrak{p}*})}(M_{\mathfrak{p}*}) \cap \mathfrak{o}_\mathfrak{p}.$$

Therefore, if we define $d_\mathfrak{p}(M)$ to be depth $M_\mathfrak{p}$ = depth $M_{\mathfrak{p}*}$, we have

$$D(M) = \prod_\mathfrak{p} \mathfrak{p}^{d_\mathfrak{p}(M)}.$$

Similarly we have

$$C(M) = \prod_{\mathfrak{p}} \mathfrak{p}^{c_{\mathfrak{p}}(M)}$$

where $c_{\mathfrak{p}}(M)$ is defined to be codepth $M_{\mathfrak{p}}$ = codepth $M_{\mathfrak{p}\mathfrak{o}}$. Some consequences of these formulas are summarized in

THEOREM 11. *An $\mathfrak{O}$-representation module is principal (coprincipal) if and only if its $\mathfrak{o}_{\mathfrak{p}}$-hull $M_{\mathfrak{p}}$ is principal (coprincipal) for every prime $\mathfrak{p}$ of $\mathfrak{o}$. If M is principal (coprincipal), then $M_{\mathfrak{p}}$ is $(\mathfrak{O}_{\mathfrak{p}}, \mathfrak{o}_{\mathfrak{p}})$-projective (injective) for all but the finitely many primes $\mathfrak{p}$ dividing $D(M)$ $(C(M))$, and M is $(\mathfrak{O}, \mathfrak{o})$-projective (injective) if and only if $M_{\mathfrak{p}}$ is $(\mathfrak{O}_{\mathfrak{p}}, \mathfrak{o}_{\mathfrak{p}})$-projective (injective) for all $\mathfrak{p}$.*

These results, together with Corollary 2 of Theorem 5 contain results of Reiner **(8)**.

We obtain in the same way that $I(\mathfrak{O}) = \Pi_{\mathfrak{p}} p^{d_{\mathfrak{p}}(\mathfrak{O})}$, where $d_{\mathfrak{p}}(\mathfrak{O})$ is defined to be depth $\mathfrak{O}_{\mathfrak{p}}$ = depth $\mathfrak{O}_{\mathfrak{p}\mathfrak{o}}$. From this, Theorem 2, and Corollary 2 to Theorem 2 we conclude that

THEOREM 12. *If $\mathfrak{O}$ has separable rational hull, $\mathfrak{O}/\mathfrak{p}\mathfrak{O}$ is a separable $\mathfrak{o}/\mathfrak{p}$-algebra for all but the finitely many primes $\mathfrak{p}$ dividing $I(\mathfrak{O})$.*

Finally we apply our results to the question of class numbers. Let S be a complete set of non-isomorphic, rationally equivalent $\mathfrak{O}$-representation modules. Then there exists an A-representation module U, $A = \mathfrak{O}_k$, such that $M_k \simeq U$ for all M in S (and we may in fact assume that M is an $\mathfrak{O}$-submodule of U for every $M \in S$). The cardinal $r = r(U)$ of the set S is called the *class number of U (with respect to $\mathfrak{O}$)*.

As was pointed out in **(2)**, Maranda's method **(7)** can be extended to prove that if A is separable, every absolutely irreducible A-representation module has finite class number, the ideal $I(\mathfrak{O}) \neq 0$ playing the role played by the group order in his arguments. On the other hand, the result of **(4)** shows the existence of non-separable semi-simple A for which every A-representation module has finite class number.

In the example of § 2, $\mathfrak{o} = Z$, the ring of rational integers, and the M_n $(n = 1, 2, \ldots,)$ are readily seen to constitute a complete set of non-isomorphic $\mathfrak{O}$-representation modules rationally equivalent to a fixed indecomposable right ideal component of A. Hence U has infinite class number. But the fact that $D(M_n) = nZ$ $(n = 1, 2, \ldots,)$ suggests the following definition for the general case: The *class number* $r(M)$ of a principal $\mathfrak{O}$-module M is defined to be the cardinal of the set S_M, where S_M is a complete set of non-isomorphic $\mathfrak{O}$-representation modules N rationally equivalent to M and such that $D(N) = D(M)$. We cannot prove here that $r(M)$ is finite when $\mathfrak{o}$ has finite ideal class number, but we reduce the problem somewhat, along the lines of the first main result of **(7)**.

Note that for an A-representation module U,

$$r(U) = \sum r(M)$$

where the sum is over a set of $M \in S$ such that $D(M)$ takes on exactly once each possible value. In the case of separable A, $I(\mathfrak{O}) \neq O$, and hence, since $D(M)$ divides $I(\mathfrak{O})$ for every M, the number of summands is finite. That the sum need not be finite in the general case is shown by the example mentioned in the preceding paragraph.

We shall say that two $\mathfrak{O}$-representation modules M and N are *equivalent at a prime* $\mathfrak{p}$ of $\mathfrak{o}$ if their $\mathfrak{o}_\mathfrak{p}$-hulls are isomorphic, or what is the same thing by Corollary 2 to Theorem 4, if their $\mathfrak{o}_{\mathfrak{p}^*}$-hulls are isomorphic. We shall say that M and N belong to the same *genus* if they are equivalent at all primes $\mathfrak{p}$ of $\mathfrak{o}$. If M is a principal $\mathfrak{O}$-module, we let

$$r_\mathfrak{p}(M) = \text{the number of classesin } S_M \text{ under equivalence at } \mathfrak{p},$$

and

$$g(M) = \text{the number of genera in } S_M.$$

From the definitions, we have $g(m) \leqslant \Pi_\mathfrak{p} r_\mathfrak{p}(M)$. By Theorems 10 and 11 we have that $r_\mathfrak{p}(M) = 1$ when $\mathfrak{p} \times \mathrm{D}(M) \cap I(\mathfrak{O}/\mathfrak{R})$, where $\mathfrak{R} = \mathfrak{O} \cap R$, R being the radical of A. Corollary 2 to Theorem 3 implies that $r_\mathfrak{p}(M)$ is finite when $\mathfrak{o}$ has finite residue class rings. Hence

THEOREM 13. *Assume that A/R is separable. Then for a principal $\mathfrak{O}$-module M, $g(M) \leqslant \Pi r_\mathfrak{p}(M)$, the product extending over the primes $\mathfrak{p}$ dividing $D(M) \cap I(\mathfrak{O}/\mathfrak{R})$, and $g(M)$ is finite if $\mathfrak{o}$ has finite residue class rings.*

For an A-module U, let $g(U)$ denote the number of genera of $\mathfrak{O}$-representation modules with rational hull isomorphic to U, and for a prime ideal $\mathfrak{p}$ of $\mathfrak{o}$, let $r_\mathfrak{p}(U)$ denote the number of classes under equivalence at $\mathfrak{p}$ of such $\mathfrak{O}$-representation modules. As was pointed out in **(2)**, if A is separable and U is absolutely irreducible, Maranda's method's **(7)** can be extended to prove that

$$g(U) = \prod_\mathfrak{p} r_\mathfrak{p}(U) \tag{1}$$

where the product extends over all prime ideals $\mathfrak{p}$ of $\mathfrak{o}$, and

$$r(U) = h \cdot g(U) \tag{2}$$

where h is the ideal class number of $\mathfrak{o}$. We leave open the general questions of when equality holds in the formula of Theorem 13, and when $r(M) = h \cdot g(M)$ for an $\mathfrak{O}$-representation module M. (See also **(9)** in this regard.)

Taking M to be a coprincipal $\mathfrak{O}$-module instead of principal, and replacing $D(M)$ by $C(M)$ in the above definitions, we obtain numbers $s(M)$, $s_\mathfrak{p}(M)$, and $h(M)$, between which relations hold analogous to those for $r(M)$, $r_\mathfrak{p}(M)$, and $g(M)$.

There are also some relations between left and right which should be mentioned. If M is an $\mathfrak{O}$-representation module, $M^+ = \text{Hom}_\mathfrak{o}(M, \mathfrak{o})$ is a left $\mathfrak{O}$-representation module, and since $\mathfrak{o}$ is a Dedekind domain, $\text{Hom}_\mathfrak{o}(M^+,\mathfrak{o}) \approx M$ and $\text{Hom}_\mathfrak{o}(M, N) \approx \text{Hom}_\mathfrak{o}(N^+, M^+)$ for $\mathfrak{O}$-representation modules M and N. Now it can be verified that $\text{Ext}^1(M, N) \approx \text{Ext}^1(N^+, M^+)$, and hence that $D(M) = C(M^+)$ and $C(M) = D(M^+)$. Moreover, relations such as $r(M) = s(M^+)$ and $g(M) = h(M^+)$ hold.

References

1. H. Cartan and S. Eilenberg, *Homological algebra* (Princeton, 1956).
2. D. G. Higman, *On orders in separable algebras*, Can. J. Math., *7* (1955), 509–515.
3. ——— *Relative cohomology*, Can. J. Math., *9* (1957), 19–34.
4. D. G. Higman and J. E. MacLaughlin, *Finiteness of class numbers of representations of algebras over function fields*, to appear in the Michigan Journal of Mathematics.
5. G. Hochschild, *Relative homological algebra*, Trans. Amer. Math. Soc., *82* (1956), 246–269.
6. J-M. Maranda, *On p-adic integral representations of finite groups*, Can. J. Math., *5* (1953), 344–355.
7. ——— *On the equivalence of representations of finite groups by groups of automorphisms of modules over Dedekind rings*, Can. J. Math., *7* (1955), 516–526.
8. I. Reiner, *Maschke modules over Dekedind rings*, Can. J. Math., *8* (1956), 329–334.
9. ——— *On class numbers of representations of an order*, A. M. S. Notices, *5* (1958), Abstract no. 548–142, 584.

University of Michigan

INTEGRAL p-adic NORMAL MATRICES SATISFYING THE INCIDENCE EQUATION

J. K. GOLDHABER

1. Introduction. The problem of arranging v elements into v sets in such a way that every set contains exactly k distinct elements and that every pair of sets has exactly $\lambda = k(k-1)/(v-1)$ elements in common, where $0 < \lambda < k < v$, is equivalent to finding a normal integral v by v matrix A such that $A^TA = B$, where B is the v by v matrix having k in every position on the main diagonal and λ in all other positions **(10)**. Utilizing the fact that for the existence of a λ, k, v design it is necessary that I (the v by v identity matrix) represent B rationally, **(2)** and **(3)** have proved the non-existence of certain λ, k, v designs. Neither of the proofs utilize the fact that it is necessary that A be normal. However, Albert **(1)** for the projective plane case and Hall and Ryser **(5)** for the general design proved that if there exists a rational A such that $A^TA = B$ then there exists a normal rational matrix satisfying the same equation. Thus the requirement of normality does not exclude any λ, k, v which were not previously excluded.

It is evident that for the existence of a λ, k, v design it is necessary that for every prime p there exist an integral p-adic normal matrix A satisfying $A^TA = B$. Assuming that $(k, k-\lambda) = 1$, we prove in § 2 that if I represents B rationally then this necessary condition is satisfied. Thus, once again, no additional designs are excluded. It does follow, however, that if I represents B rationally then I represents B without essential denominator and, furthermore, that there is a form in the genus of I which represents B integrally.

In § 3 we consider a modified incidence equation which is satisfied by every incidence matrix and which, if I represents B rationally, has integral solutions. Sufficient conditions for the existence of a λ, k v design in terms of these integral solutions are given.

2. The incidence equation examined locally. We assume throughout this paper that $(k, k-\lambda) = 1$. Thus, since $\lambda v = k^2 - (k-\lambda)$ we have $(\lambda, k) = (\lambda, k-\lambda) = (v, k) = (v, k-\lambda) = 1$. The matrices I and B are as above. We prove

THEOREM 1. *If I represents B rationally then for every prime p there exists a matrix A with elements in the ring $R(p)$ of p-adic integers such that $A^TA = AA^T = B$.*

Received November 3, 1958. Research supported in part by the Office of Ordinance Research under Contract DA-23-072-ORD-1051.

We show first that there exists a matrix C (not necessarily normal) with elements in $R(p)$ such that $C^TC = B$. It follows from well-known theorems on quadratic forms **(7)** and the fact that I and B are both positive definite that it is sufficient to show this for all primes $p \in P$, where P is the set of all prime divisors of $2 \cdot \det B = 2k^2(k - \lambda)^{v-1}$. Let T be the v by v matrix

$$\begin{bmatrix} 1 & -1 & -1 & -1 & -1 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 1 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Then

$$T^TT = \begin{bmatrix} v & 0 \\ 0 & I_1 + S_1 \end{bmatrix}$$

where I_1 is the $(v - 1)$ by $(v - 1)$ identity matrix and S_1 is the $(v - 1)$ by $(v - 1)$ matrix each of whose entries is 1. Also,

$$T^TBT = \begin{bmatrix} k^2v & 0 \\ 0 & (k - \lambda)(I_1 + S_1) \end{bmatrix}.$$

Since $(k, k - \lambda) = 1$, v is a p-adic unit for all odd $p \in P$. v is also a 2-adic unit in the case that v is odd. Hence, for odd p, $X^TX = B$ is solvable in $R(p)$, $p \in P$, if and only if $X^T(T^TT)X = T^TBT$ is solvable in $R(p)$; and for odd v, $X^TX = B$ is solvable in $R(2)$ if and only if $X^T(T^TT)X = T^TBT$ is solvable in $R(2)$.

We first dispose of the case when v is even. Since I represents B rationally, $(k - \lambda)$ is a square **(3)**; whence, obviously T^TT represents T^TBT in $R(p)$ for all odd $p \in P$. Furthermore, since v is even and $(k, k - \lambda) = 1$ it follows that k and $k - \lambda$ are both odd. Thus I and B are properly primitive forms (that is, each has a 2-adic unit element on its main diagonal) with unit 2-adic determinants which, since they are rationally congruent, are congruent over the 2-adic field. Hence **(7**, Theorem 36**)** they are equivalent in $R(2)$. Thus, if v is even I represents B in $R(p)$ all $p \in P$.

Suppose now that v is odd. It is clearly sufficient to show that $I_1 + S_1$ represents $(k - \lambda)(I_1 + S_1)$ in $R(p)$ for all $p \in P$.

(i) $I_1 + S_1$ represents $(k - \lambda)(I_1 + S_1)$ in $R(2)$.

(a) Suppose $(k - \lambda) = 2^{2b}m$ where $b \geqslant 0$ and m is odd. We make use here, and below, of the following known theorem **(6)**:

Two improperly primitive forms (that is, each form has some 2-adic unit element but no 2-adic unit element on its main diagonal) in the same number

of variables and of odd determinants are equivalent in $R(2)$ if and only if their determinants are congruent mod 8.

From this it follows that $I_1 + S_1$ and $m(I_1 + S_1)$ are equivalent in $R(2)$. But then, obviously, $I_1 + S_1$ represents $2^{2b}\, m(I_1 + S_1)$ in $R(2)$.

(b) Suppose $k - \lambda = 2^{2b+1}m$ where m is odd. We shall show below that in this case the assumption that I represents B rationally implies that $v = \pm 1$ mod 8.

If $v \equiv 1$ mod 8 then $I_1 + S_1$ and $m(I_1 + S_1)$ are both equivalent to the $\frac{1}{2}(v-1)$ fold direct sum of the matrix

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

Call the direct sum matrix K. It is thus sufficient to show that K represents $2^{2b+1}K$. Since $v \equiv 1$ mod 8, $4|v-1$. Let L be the $\frac{1}{4}(v-1)$ fold direct sum of

$$\begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & -1 & 0 \end{bmatrix}.$$

Then $(2^bL)^T K(2^bL) = 2^{b+1}K$ as desired.

If $v \equiv -1$ mod 8 then $I_1 + S_1$ and $m(I_1 + S_1)$ are both equivalent in $R(2)$ to $K_1 \oplus K_2$. Here $\oplus$ denotes direct sum, K_1 is the $\frac{1}{2}(v-7)$ fold direct sum of

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

and K_2 is the 6 by 6 matrix having each entry on its main diagonal equal to 2 and all other entries equal to 1. Note that $4|v-7$. Let L_1 be the $\frac{1}{4}(v-7)$ fold direct sum of the 4 by 4 matrix given in the preceding paragraph, and let L_2 be the matrix

$$\begin{bmatrix} -1 & 0 & -1 & -1 & -1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 \\ -1 & -1 & -1 & 0 & 0 & -1 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \end{bmatrix}.$$

Then $[2^b(L_1 \oplus L_2)]^T (K_1 \oplus K_2)[2^b(L_1 \oplus L_2)] = 2^{2b+1}(K_1 \oplus K_2)$; whence, $I_1 + S_1$ represents $(k-\lambda)(I_1 + S_1)$ in $R(2)$ as desired.

It remains to show that if I represents B rationally and if $k - \lambda = 2^{2b+1}m$, m odd, then $v \equiv \pm 1$ mod 8. Since $\lambda v = k^2 - (k-\lambda)$ we have

$$\left(\frac{k-\lambda}{\lambda}\right) = \left(\frac{2}{\lambda}\right)\left(\frac{m}{\lambda}\right) = 1,$$

where (a/b) is the Jacobi symbol. (Since $(k, k-\lambda) = 1$, λ is odd.) We thus have

$$\left(\frac{\lambda}{m}\right) = \left(\frac{2}{\lambda}\right)(-1)^{\frac{m-1}{2}\cdot\frac{\lambda-1}{2}}.$$

We consider the cases $b \geqslant 1$, $b = 0$ separately.

If $b \geqslant 1$ then $\lambda \equiv v \bmod 8$. If $v = 3 \bmod 8$ then $(-\lambda/m) = -1$ but this is impossible since I represents B rationally **(3)**. The case $v \equiv 5 \bmod 8$ is disposed of similarly.

If $b = 0$ then $\lambda v \equiv -1$ or $3 \bmod 8$ according as $k - \lambda \equiv 2$ or $6 \bmod 8$. If $k - \lambda \equiv 2 \bmod 8$ and $v \equiv 3 \bmod 8$ then $(-\lambda/m) = -1$ which is impossible. Similar easy computations exclude all possibilities other than $v \equiv \pm 1 \bmod 8$.

(ii) $I_1 + S_1$ represents $(k-\lambda)(I_1 + S_1)$ in $R(p)$ for all odd p such that $p|k$.

We make use here, and below, of the following known theorem **(6, 11)**.

For odd p, two forms, f and g, in the same number of variables and of unit determinants in $R(p)$ are equivalent in $R(p)$ if and only if

$$\left(\frac{\det f}{p}\right) = \left(\frac{\det g}{p}\right).$$

The desired result is an immediate consequence of this theorem. We actually have somewhat more; namely, $I_1 + S_1$ represents $(k-\lambda)(I_1 + S_1)$ in $R(p)$ for all odd p such that $p \nmid (k-\lambda)v$.

(iii) $I_1 + S_1$ represents $(k-\lambda)(I_1 + S_1)$ in $R(p)$ for all odd p such that $p|(k-\lambda)$. Suppose $(k-\lambda) = p^b m$ where $(p, m) = 1$ and $b > 0$. We consider two cases: (*a*) $v \equiv 1 \bmod 4$, and (*b*) $v \equiv 3 \bmod 4$.

(a) Since I represents B rationally we must have $(v/p) = (\lambda/p) = 1$, **(2)**. Thus $\det(I_1 + S_1) = v$ and $\det[m(I_1 + S_1)] = m^{s-1}v$ are both units and perfect squares in $R(p)$. Therefore, $I_1 + S_1$ and $m(I_1 + S_1)$ are both equivalent in $R(p)$ to I_1. It is thus sufficient to show that I_1 represents $p^b I_1$ in $R(p)$. If b is even, this is obvious. Suppose then that $b = 2c + 1$. We use the device employed in **(3)**. There exist integers a_i, $i = 1, 2, 3, 4$, such that $\sum_1^4 a_i^2 = p$. Let L be the $\frac{1}{4}(v-1)$ fold direct sum of

$$p^c \cdot \begin{bmatrix} a_1 & a_2 & a_3 & a_4 \\ a_2 & -a_1 & -a_4 & a_3 \\ a_3 & a_4 & -a_1 & -a_2 \\ a_4 & -a_3 & a_2 & -a_1 \end{bmatrix}.$$

Then $L^T L = p^{2c+1} I_1$ as desired.

(b) For $v \equiv 3 \bmod 4$ we must have

$$\left(\frac{v}{p}\right) = \left(\frac{\lambda}{p}\right) = (-1)^{\frac{p-1}{2}},$$

(3). Thus $I_1 + S_1$ and $m(I_1 + S_1)$ are both equivalent to the $(v-1)$ $(v-1)$ diagonal matrix $[1, 1, \ldots, 1, (-1)^{\frac{1}{2}p-\frac{1}{2}}] = J$. We must show that J represents $p^b J$. For even b this is obvious and so we may take $b = 2c+1$. If $p \equiv 3 \bmod 4$ then let L_1 be the $\frac{1}{4}(v-3)$ fold direct sum of the 4 by 4 matrix given in the previous paragraph and let

$$L_2 = p^c \begin{bmatrix} a & 1 \\ 1 & a \end{bmatrix}$$

where a is a p-adic integer such that $a^2 = 1 + p$. Then $[(L_1 \oplus L_2)]^T J[(L_1 \oplus L_2)] = p^b J$. If $p = 1 \bmod 4$ then there exist integers a_1 and a_2 such that $a_1^2 + a_2^2 = p$. Let L be the $\frac{1}{2}(v-1)$ fold direct sum of

$$p^c \begin{bmatrix} a_1 & a_2 \\ a_2 & -a_1 \end{bmatrix}.$$

Then $L^T J L = p^b J$.

It follows from all the above that for every p there exists a matrix C with elements in $R(p)$ such that $C^T C = B$. It remains to show that there exists a normal matrix with the desired properties. If $p \nmid v$ this is clear. In fact, we have seen above that for every $p \nmid v$ there exists a C_1 with elements in $R(p)$ such that $C_1^T (I_1 + S_1) C_1 = (k-\lambda)(I_1 + S_1)$. Let $A = T(k \oplus C_1) T^{-1}$. Then $A^T A = B$ and $AS = kS$, where S is the v by v matrix composed entirely of ones; whence by **(5**, Theorem 3.1**)** A is normal. Since $p \nmid v$, A has its elements in $R(p)$.

Suppose $p|v$. We know that there exists a matrix $C = (c_{ij})$ with elements in $R(p)$ such that $C^T C = B$. Let α be the column vector $[r_1, r_2, \ldots, r_v]$ where $r_i = \sum_j c_{ij}$, and let β be the v by 1 column vector each of whose entries is k. We will show that there exists an orthogonal matrix O with elements in $R(p)$ such that $O\alpha = \beta$. It will follow that $A = OC$ is such that $A^T A = B$, $AS = kS$; and again by **(5)**, A is normal as desired.

We use the following theorem **(4**, Satz 10.4**)**. It is stated here more concretely and in a less general form that in **(4)**.

Let V be a v dimensional vector space of column vectors over the p-adic field with a non-degenerate ground form given by the v by v symmetric matrix G. Let $\mathfrak{F}$ be a lattice in V and let $\mathfrak{D}$ be its different. If α and β are primitive vectors in $\mathfrak{F}$ such that $\alpha^T G \alpha = \beta^T G \beta$ and $\alpha - \beta \in \mathfrak{D}$ then there exists a v by v matrix O with elements in $R(p)$ such that $O^T G O = G$ and $O\alpha = \beta$.

For our purposes we take G to be the identity matrix, $\mathfrak{F}$ as the lattice which has as a basis the column vectors of the identity matrix I, and α and β as above. We note that if p is odd then $\mathfrak{D} = \mathfrak{F}$, and if $p = 2$ then $\mathfrak{D}$ is the lattice which has as a basis the column vectors of $2I$. From the fact that $C^T C = B$ it follows easily **(10)** that $\sum_j c_{ji} r_j = k^2$ and $\sum_i r_i^2 = k^2 v$. From the first of the latter equations and the facts that $p|v$, $(k, v) = 1$ it follows that α and β are both primitive. From the second of these equations it follows that $\alpha^T \alpha = \beta^T \beta$. Hence if p is odd the desired O exists.

In order to complete the proof for $p = 2$ it is sufficient to show that $r_i^2 \equiv 1 \bmod 2$. Let t_{ij} be the inner product of the ith and jth rows of C. Again as in **(10)** we have

$$k^2 t_{ij} = \lambda r_i r_j + k^2(k - \lambda)\,\delta_{ij}.$$

If $r_i^2 \equiv 0 \bmod 2$ then $t_{ii} \equiv 1 \bmod 2$ and we would have

$$0 \equiv r_i^2 \equiv \sum_j c_{ij}^2 = t_{ii} \equiv 1 \bmod 2$$

which is clearly absurd.

This completes the proof of Theorem 1.

As immediate consequences we have

COROLLARY 1. *If I represents B over the rational field then I represents B rationally without essential denominator, that is, for every positive integer m there is a matrix D with rational elements whose denominators are prime to m such that $D^T D = B$.*

COROLLARY 2. *If I represents B rationally then there exists a form in the genus of I which represents B integrally.*

3. A modified incidence equation. Since the genus of the identity contains more than one class for $v > 8$ **(8)** Corollary 2 does not yield any new designs. It is natural, therefore, to examine a matric equation, akin to $X^T X = B$, which is still satisfied by every incidence matrix, has integral solutions, and then to examine the relationship of these integral solutions to incidence matrices.

THEOREM 2. *Let $t = a/b$ be a rational number greater than $1/v$ such that $(av - b)b$ is odd. Let S be the v by v matrix composed entirely of ones. If I represents B rationally then $I - tS$ represents $B - tk^2 S$ integrally.*

For by Theorem 1, $bI - aS$ represents $bB - ak^2 S$ in every $R(p)$. (The normality of A implies that $SA = AS = kS$ and therefore $A^T(bI - aS)\,A = bB - ak^2 S$.) Hence there exists a form in the genus of $bI - aS$ which represents $bB - ak^2 S$ integrally. Since the genus of an indefinite form of odd determinant in $v > 2$ variables consists of exactly one class **(9)** Theorem 2 follows.

Let $\mathcal{S}$ be the set of all rationals which have the properties stated in Theorem 2. For $t \in \mathcal{S}$ let $A(t) = (a_{ij}(t))$ denote an arbitrary but fixed integral solution of $X^T(I - tS)X = B - tk^2 S$. Let $r_i(t) = \sum_j a_{ij}(t)$, and $s_j(t) = \sum_i a_{ij}(t)$.

THEOREM 3: (i) *If $A(t_0)$ is normal and $t_0 \neq (k + (k - \lambda)^{\frac{1}{2}})/kv$ then $A(t_0)$ is an incidence matrix or the negative of one.*

(ii) *If for $t_1, t_2 \in \mathcal{S}$, $t_1 \neq t_2$ we have $r_i(t_1) = r_i(t_2)$ $(s_i(t_1) = s_i(t_2))$ for $i = 1, 2, 3, \ldots, v$, then $A(t_1)$ is an incidence matrix or the negative of one.*

(iii) *If there exists an M and a subset $\mathcal{S}'$ of $\mathcal{S}$ containing sufficiently many distinct elements (see below) such that $|r_i(t)| < M (|s_i(t)| < M)$ for $t \in \mathcal{S}'$ and*

$i = 1, 2, \ldots, v$ then there exists a $t_0 \in \mathscr{S}'$ such that $A(t_0)$ is an incidence matrix or the negative of one.

(iv) *If $r_i(t_0) > 0$ for $i = 1, 2, \ldots, v$ and for $t_0 > 1$ then $A(t_0)$ is an incidence matrix.*

(i) As in **(10)** the following relations may be established: For every $t \in \mathscr{S}$,

$$\sum r_i^2(t) - t\Big(\sum r_i(t)\Big)^2 = k^2v(1 - tv)$$

$$k^2(1 - tv)\Big(\sum s_i^2(t)\Big) + (k^2t - \lambda)\Big(\sum r_i(t)\Big)^2 = k^2(k - \lambda)v.$$

Now the normality of $A(t_0)$ implies that $\sum r_i^2(t_0) = \sum s_i^2(t_0)$. Since $t_0 \neq (k + (k - \lambda)^{\frac{1}{2}})/kv$, the above equations imply that $\sum r_i^2(t_0) = k^2v$ and $\sum s_i(t_0) = \sum r_i(t_0) = \pm kv$. Whence $r_i(t_0) = s_i(t_0) = k$ or $r_i(t_0) = s_i(t_0) = -k$ for all i. But then $A^TA = AA^T = B$ and the result follows by **(10**, Theorem 2.1**)**.

(ii) The proof of this result is analogous to the proof of (i).

(iii) The number of lattice points in v dimensional space over the reals with components having absolute value less than M is finite. Hence if $\mathscr{S}'$ contains more elements than the number of such lattice points then there exist t_1, $t_2 \in \mathscr{S}'$, $t_1 \neq t_2$, such that $r_i(t_1) = r_i(t_2)$ for $i = 1, 2, \ldots, v$. The desired result follows from (ii).

(iv) Once again as in **(10)** it may be shown that $r_i(t) \equiv 0 \bmod k$. Since $r_i(t) > 0$ it follows that

$$\Big(\sum r_i(t)\Big)^2 > \Big(\sum r_i^2(t)\Big) + v(v - 1)k^2.$$

From the first of the equation given in (i) above it follows that

$$k^2v(1 - t) \leqslant (1 - t) \sum r_i^2(t).$$

Since $t > 1$ we have $\sum r_i^2(t) \leqslant k^2v$. But also

$$k^2v^2 \leqslant (\sum r_i(t))^2 \leqslant v(\sum r_i^2(t)).$$

Hence $\sum r_i^2(t) = k^2v$ and the proof may be completed as was the proof of (i).

We remark that if $v > k + 1$ and $t > 1$ then $r_i(t) \neq 0$ for $i = 1, 2, \ldots, v$.

Theorem 3 gives sufficient conditions for the existence of a λ, k, v design in terms of integral solutions, which by Theorem 2 are known to exist, of the matric equation

$$X^T(I - tS)X = B - tk^2S.$$

The problem of determining the nature of these solutions appears to be extremely difficult. Also of interest, and possibly a more pliable problem, is the determination of the integral automorphs of $I - tS$ and $B - tk^2S$.

References

1. A. A. Albert, *Rational normal matrices satisfying the incidence equation*, Proc. Amer. Math. Soc., *4* (1953), 554–9.
2. R. H. Bruck and H. J. Ryser, *The nonexistence of certain finite projective planes*, Can. J. Math., *1* (1949), 88–93.
3. S. Chowla and H. J. Ryser, *Combinational problems*, Can. J. Math., *2* (1950), 93–9.
4. M. Eichler, *Quadratische formen und orthogonale gruppen* (Berlin, 1952).
5. Marshall Hall and H. J. Ryser, *Normal completions of incidence matrices*, Amer. J. Math., *76* (1954), 581–9.
6. B. W. Jones, *A canonical quadratic form for the ring of 2-adic integers*, Duke Math. J., *11* (1944), 715–27.
7. ——— *The arithmetic theory of quadratic forms*, Carus Math. Monographs, *10* (1950).
8. W. Magnus, *Ueber die Anzahl der in einem Geschlecht enthaltenen Klassen von positiv definiten quadratischen Formen*, Math. Ann. *114* (1937), 465–75.
9. A. Mayer, Zürich naturf. Ges., *36* (1891), 241.
10. H. J. Ryser, *Matrices with integer elements in combinational investigations*, Amer. J. Math., *74* (1952), 769–73.
11. C. L. Siegel, *Equivalence of quadratic forms*, Amer. J. Math. *63* (1941), 658–80.

Washington University

LOOPS WITH ADJOINTS

W. R. COWELL

Introduction. It is shown in **(6)** how to represent certain sets of orthogonal Latin squares as a group together with a set of permutations of the group elements. The correspondence between 3-nets and loops is well known; for example, see **(8)**. We shall consider a loop G together with a certain set of permutations on the elements of G and shall interpret such a structure as an incidence system in which the 3-net of the loop is embedded. Specifically, the permutations or "adjoints" will give rise to lines which may be adjoined to the 3-net of G in the sense of **(3)**. The group of autotopisms of the loop determines a group of automorphisms of its 3-net analogous to collineations in an affine plane. We shall study the problem of extending these incidence preserving mappings to the adjoined lines. By analogy with the study of loops with operators, we shall consider homomorphisms of loops with adjoints and examine geometric consequences. Particular attention will be paid to the case where G has the inverse property and the adjoints are "linear." The special case in which G is an abelian group is of geometric interest in that the corresponding incidence systems include the Veblen-Wedderburn affine planes.

1. Nets, loops, and adjoints. A *net* $\mathfrak{N}$ is a set of undefined objects called "points" and "lines," together with a symmetric incidence relation (point on line, line through point), such that the lines can be partitioned into non-empty, disjoint subsets called "parallel classes" and the following incidence axioms hold:

(i) Any point of $\mathfrak{N}$ lies on exactly one line of each parallel class.

(ii) Any pair of lines from distinct classes have exactly one point in common.

(iii) There are at least three distinct parallel classes.

An *affine plane* is a net which satisfies

(iv) Given two distinct points of $\mathfrak{N}$, there is a unique line containing both of them.

(v) There exists a set of four distinct points of $\mathfrak{N}$, no three of which lie on the same line.

If a net $\mathfrak{N}$ possesses a finite number k of parallel classes, one refers to $\mathfrak{N}$ as a k-net.

Suppose L is a set of points of the net $\mathfrak{N}$ such that if M is any line of $\mathfrak{N}$,

Received August 16, 1958.

then L contains exactly one point of M. We say that L may be "adjoined as a line to $\mathfrak{N}$."

Let $(G, +)$ be a loop. By the 3-net associated with G we mean the net $\mathfrak{N}(G)$ whose points are ordered pairs (x, y), x and y in G, and whose three classes of lines are given by $x = c$, $y = c$, and $y = x + c$ where c ranges over G and incidence means satisfaction of the equation.

Let ϵ be the identity map on the loop G. An *adjoint* of G is a permutation σ on G for which there exists a permutation τ on G such that $\epsilon + \tau = \sigma$, where addition of mappings is defined by adding images. The permutation τ is a "complete mapping" in the sense of **(6)** and will be called the *companion* of σ.

THEOREM 1. *A line L can be adjoined to $\mathfrak{N}(G)$ if and only if G possesses an adjoint σ.*

Proof. Suppose σ is an adjoint of G with companion τ. Define L to be the set of points $(x, x\sigma)$, $x \in G$. If $c \in G$ then L contains exactly the point $(c, c\sigma)$ of the line $x = c$, the point $(c\sigma^{-1}, c)$ of the line $y = c$, and the point $(c\tau^{-1}, c\tau^{-1}\sigma)$ of the line $y = x + c$. Thus L may be adjoined to $\mathfrak{N}(G)$.

Conversely, let L be a set of points which is adjoined as a line to $\mathfrak{N}(G)$. If $(a, b) \in L$, define $a\sigma = b$. Since L contains exactly one point from each line $x = c$ and each line $y = c$, we see that σ is a permutation on G. Define the mapping τ of G into G by the equation $a\sigma = a + a\tau$, $a \in G$. For each $c \in G$, the line $y = x + c$ passes through exactly one point $(a, a\sigma)$ of L. Hence τ is a permutation and σ is an adjoint of G.

The incidence system consisting of $\mathfrak{N}(G)$ together with the adjoined lines associated with a set Σ of adjoints of G will be called the *quasinet* $\mathfrak{Q}(G, \Sigma)$.

A set Σ of adjoints of G is said to be *compatible* if, for every distinct pair σ_1, σ_2 in Σ, there is at most one $x \in G$ such that $x\sigma_1 = x\sigma_2$; that is, the corresponding lines of $\mathfrak{Q}(G, \Sigma)$ share at most one point.

2. Adjoints under isotopy. The loops $(G, +)$ and $(G, \oplus)$ defined on the same set G are said to be *isotopic* if there exists an ordered triple (α, γ, β) of permutations of G such that $x\alpha \oplus y\gamma = (x + y)\beta$. We write $(G, +) = (\alpha, \gamma, \beta)(G, \oplus)$. If $\oplus$ is the same operation as $+$ then (α, γ, β) is called an *autotopism* of $(G, +)$. Isotopy is an equivalence relation on the set of all loops and the autotopisms of a loop form a group which contains the automorphism group of G. We refer the reader to **(2)** for a discussion of the algebraic properties of isotopy and autotopy.

A *homomorphism* of a net $\mathfrak{N}$ onto a net $\mathfrak{N}'$ is a mapping of points onto points and lines onto lines which preserves incidence and parallelism and is one-one on classes of lines. If the homomorphism is one-one on points and lines, it is called an *isomorphism*.

The proofs of the following two well-known theorems may essentially be found in **(8)**.

THEOREM 2. *The mapping*

$$(x, y) \to (x\alpha, y\beta)$$
$$[x = c] \to [x = c\alpha]$$
$$[y = c] \to [y = c\beta]$$
$$[y = x + c] \to [y = x \oplus c\gamma]$$

is an isomorphism of $\mathfrak{N}(G, +)$ *onto* $\mathfrak{N}(G, \oplus)$ *if and only if* $(G, +) = (\alpha, \gamma, \beta)(G, \oplus)$.

THEOREM 3. *Let* $\mathfrak{N}$ *be an arbitrary 3-net and let* O *be a point of* $\mathfrak{N}$. *Let the designations* $x = c$, $y = c$, *and* $y = x + c$ *be assigned to the three classes. Then, for some appropriate loop* G, $\mathfrak{N} = \mathfrak{N}(G)$, O *is the point* $(0, 0)$, *and the three classes are as designated. Moreover, if a different point* O' *is chosen and the class designation remains the same, then* $\mathfrak{N} = \mathfrak{N}(G')$ *for some* G' *isotopic to* G.

It is clear that isomorphic nets have corresponding adjoined lines; thus isotopic loops have corresponding adjoints. The correspondence is given in the proof of

THEOREM 4. *Let* $(G, +)$ *be a loop with an adjoint* σ. *Suppose* $(G, +) = (\alpha, \gamma, \beta)(G, \oplus)$. *Then* $(G, \oplus)$ *possesses a unique adjoint* σ' *so that the isomorphism of Theorem 2 can be extended to an incidence preserving mapping of the associated adjoined lines.*

Proof. The set of images of the points $(x, x\sigma)$, $x \in G$ is a line adjoined to $\mathfrak{N}(G, \oplus)$ if and only if $(x\alpha, x\sigma\beta) = (x\alpha, x\alpha\sigma')$ for each x where σ' is an adjoint of $(G, \oplus)$. If the condition holds,then $\sigma' = \alpha^{-1}\sigma\beta$ and we show that this σ' is an adjoint for (G, $\oplus$). Let σ have companion τ. Then, for all $x \in G$,

$$x(\epsilon \oplus \alpha^{-1}\tau\gamma) = x\alpha^{-1}\alpha(\epsilon \oplus \alpha^{-1}\tau\gamma) = (x\alpha^{-1})\alpha \oplus (x\alpha^{-1}\tau)\gamma =$$
$$(x\alpha^{-1} + x\alpha^{-1}\tau)\beta = x\alpha^{-1}(\epsilon + \tau)\beta = x\alpha^{-1}\sigma\beta.$$

Thus the companion of $\alpha^{-1}\sigma\beta$ is $\alpha^{-1}\tau\gamma$.

If $V = (\alpha, \gamma, \beta)$ is an autotopism of a loop G and Σ is a set of adjoints of G, then we say that V is *extensible* relative to Σ if $\alpha^{-1}\Sigma\beta = \Sigma$. From the proof of Theorem 4, we see that the extensible autotopisms are exactly those for which the automorphism of $\mathfrak{N}(G)$ given by Theorem 2 induces a line onto line, incidence preserving mapping of $\mathfrak{N}(G, \Sigma)$.

An example of an extensible autotopism is furnished by a projective plane with a collineation which leaves fixed every point of some line $\mathscr{L}$. Let $\mathscr{L}$ be used as the line at infinity and construct a co-ordinate system as in (4). Take G to be the additive loop of the ternary and let Σ be the set of mappings $x \to x \,.\, m \circ b$ where m assumes some set of values exclusive of $0, 1, \infty$, and where b takes on all values from the ternary for each m. The collineation then induces an automorphism of $\mathfrak{N}(G)$ corresponding to an autotopism of G which is extensible relative to Σ by virtue of the fact that adjoined lines are mapped into adjoined lines.

3. Homomorphisms. Let H be a normal subloop of G and let η be the natural homomorphism of G onto G/H. Then we may define a homomorphism of $\mathfrak{N}(G)$ onto $\mathfrak{N}(G/H)$ by a mapping of the same form as that used in Theorem 2 with $\alpha = \beta = \gamma = \eta$ and $\oplus$ taken as $+$, the operation in G/H. Furthermore, it follows easily from Theorem 3 that every homomorphism of a 3-net onto a 3-net can be viewed in this way for appropriate G and H.

Suppose σ is an adjoint of G with companion τ. A normal subloop H of G is a *σ-subloop* provided any one of the following implies the other two: (i) $x \equiv y \bmod H$, (ii) $x\sigma \equiv y\sigma \bmod H$, (iii) $x\tau \equiv y\tau \bmod H$. If Σ is a set of adjoints, then H is a normal Σ-subloop if H is a normal σ-subloop for each $\sigma \in \Sigma$. This definition states that σ^* defined by $(x + H)\sigma^* = x\sigma + H$ is a permutation of G/H. The same statement applies to τ^* and, moreover, $(x + H)(\epsilon^* + \tau^*) = (x + H) + (x + H)\tau^* = (x + H) + (x\tau + H) = (x + x\tau) + H = x\sigma + H = (x + H)\sigma^*$ for all x and thus σ^* is an adjoint of G/H. Furthermore, the point $(x, x\sigma)$ maps into $(x + H, (x + H)\sigma^*)$ so the adjoined line of $\mathfrak{N}(G)$ defined by σ maps onto the adjoined line of $\mathfrak{N}(G/H)$ defined by σ^*.

Suppose, conversely, that H is normal in G, that σ is an adjoint of G, and that the images $(x + H, x\sigma + H)$ form a line adjoined to $\mathfrak{N}(G/H)$. Then the mapping $x + H \to x\sigma + H$ is an adjoint of G/H. Hence, $x + H = y + H$ if and only if $x\sigma + H = y\sigma + H$. Also, if $x' + H$ is the unique solution of $(x + H) + (x' + H) = x\sigma + H$, then $x + H \to x' + H$ is a permutation of G/H so $x + H = y + H$ if and only if $x' + H = y' + H$. But $x\sigma + H = (x + x') + H = (x + x\tau) + H$ so $x' + H = x\tau + H$. Therefore, H is a normal σ-subloop of G.

4. Linear adjoints and extensibility. If $a \in G$, the permutation $\rho(a)$ is defined by $x\rho(a) = x + a$. A permutation of G is *linear* if it has the form $\sigma = \delta\rho(a)$ where δ is an automorphism of G. We say that σ is *strongly linear* if a is in the associator **(see 2)** of G. An adjoint σ of G is linear (strongly linear) if *both* σ and its companion are linear (strongly linear) as permutations. If a linear adjoint σ has $a = 0$, σ is an *automorphism adjoint.*

LEMMA 1. (i) *If $\sigma = \delta\rho(a)$ is a linear adjoint with companion $\gamma\rho(b)$ then $a = b$. If σ is strongly linear, then δ is a strongly linear adjoint with companion γ.*

(ii) *If σ is any adjoint on G with companion τ and a is in the associator of G then $\sigma\rho(a)$ is an adjoint with companion $\tau\rho(a)$.*

Proof. (i) $0(\epsilon + \gamma\rho(b)) = 0\delta\rho(a)$ gives $a = b$. Under strong linearity, $x\delta + a = x + (x\gamma + a) = (x + x\gamma) + a$ for every $x \in G$ and thus $\delta = \epsilon + \gamma$.

(ii) $x(\epsilon + \tau\rho(a)) = x + (x\tau + a) = (x + x\tau) + a = x\sigma\rho(a)$.

A set Σ of strongly linear adjoints of G will be called *complete* if, for every automorphism δ such that $\delta\rho(a) \in \Sigma$, $\delta\rho(b) \in \Sigma$ for every b in the associator of G. Lemma 1 guarantees that $\delta\rho(b)$ is an adjoint.

Bruck **(2**, ch. II, § 4**)** has studied three types of autotopisms of a com-

mutative loop G with the inverse property and has shown that these autotopisms generate the autotopism group of G. The following theorem shows that certain subclasses of types (1) and (2) and all autotopisms of type (3) are extensible relative to a complete set of strongly linear adjoints.

THEOREM 5. *Suppose G is a commutative loop with the inverse property and Σ is a complete set of strongly linear adjoints of G.*

(i) *If $U = (\alpha, \alpha, \alpha)$ where α is an automorphism of G, then U is extensible relative to Σ if and only if $\alpha^{-1}\Delta\alpha = \Delta$ where Δ is the set of automorphisms in Σ.*

(ii) *If $V = (\rho(a), \rho(a), \rho(a)^2)$ where a is in the associator of G, then V and all the autotopisms obtainable from V by Bruck's Lemma 4A are extensible relative to Σ.*

(iii) *If $W = (\epsilon, \rho(a), \rho(a))$ where ϵ is the identity and a is in the associator of G, then W and all the autotopisms obtainable from W by Bruck's Lemma 4A are extensible relative to Σ.*

Proof. (i) Suppose U is extensible. Let $\delta\rho(b) \in \Sigma$. Then, for all $x \in G$, $x\alpha^{-1}\delta\rho(b)\alpha = x\alpha^{-1}\delta\alpha + b\alpha = x\gamma + c$ for some $\gamma \in \Delta$, c an associator element. If $x = 0$, $b\alpha = c$ and $\alpha^{-1}\delta\alpha = \gamma$. Similarly $\alpha\Delta\alpha^{-1} \subseteq \Delta$.

Conversely, assume $\alpha^{-1}\Delta\alpha = \Delta$. Then, if $x \in G$, $x\alpha^{-1}\delta\rho(a)\alpha = x(\alpha^{-1}\delta\alpha)\rho(a\alpha)$ and $x\alpha\delta\rho(a)\alpha^{-1} = x(a\delta\alpha^{-1})\rho(a\alpha^{-1})$. Since the associator is a characteristic subloop of G, U is extensible.

(ii) Consider $x\rho(a)^{-1}\delta\rho(b)\rho(a)^2 = [(x - a)\delta + b] + 2a = x\delta\rho(c)$ where c is in the associator. Similarly, $\rho(a)\delta\rho(b)\rho(a)^{-2} \in \Sigma$.

Extensibility for the autotopisms obtained by using Bruck's Lemma 4A may be verified with a certain amount of similar computation.

(iii) We compute $x\epsilon^{-1}\delta\rho(b)\rho(a) = (x\delta + b) + a = x\delta\rho(c)$ and $x\epsilon\delta\rho(b)\rho(a)^{-1} = (x\delta + b) - a = x\delta\rho(d)$ where c and d are in the associator.

Again, it is straightforward to verify that the "derived" autotopisms are extensible.

THEOREM 6. *Let G be an abelian group and let Σ be a complete set of (strongly) linear adjoints of G. If Δ is the set of automorphisms in Σ, let $\delta_1 - \delta_2$ be a permutation (and hence an automorphism) of G for every pair $\delta_1, \delta_2 \in \Delta$, $\delta_1 \neq \delta_2$. Then, the quasinet $\mathfrak{Q}(G, \Sigma)$ is a net each of whose parallel classes, besides those of $\mathfrak{N}(G)$, consists of the set of adjoined lines given by the adjoints $\delta\rho(c)$ where δ is fixed and c ranges over G. Moreover, the automorphisms of $\mathfrak{Q}(G, \Sigma)$ are exactly given by $(x, y) \to (x\alpha + r, y\alpha + s)$ where α is an automorphism of G in the centralizer of Δ and r, s are in G.*

Proof. The point $(a, b) \in \mathfrak{Q}(G, \Sigma)$ is on exactly the line determined by $\delta\rho(c)$, $c = b - a\delta$, in the class corresponding to δ. Any line from an adjoined class contains exactly one point in common with each line of $\mathfrak{N}(G)$ and thus we need only consider lines determined by $\delta_1\rho(a)$, $\delta_2\rho(b)$ where $\delta_1 \neq \delta_2$. It is easy to see that these lines share exactly the point (x, y) where $x = (b - a)(\delta_1 - \delta_2)^{-1}$, $y = x\delta_1\rho(a) = x\delta_2\rho(b)$. Hence $\mathfrak{Q}(G, \Sigma)$ is a net.

Every automorphism of the net $\mathfrak{Q}(G, \Sigma)$ induces an automorphism of $\mathfrak{N}(G)$ which, by virtue of Theorem 2, corresponds to an autotopism of G. By Bruck's Theorem 4D **(2**, ch. II, § 4**)**, this autotopism is of the form UVW where U, V, and W are of types (i), (ii), (iii) respectively, as described in Theorem 5. It is easy to check that V and W and hence VW correspond to "translations": $(x, y) \to (x + r, y + s)$. Thus, the autotopism UVW corresponds to $(x, y) \to (x\alpha + r, y\alpha + s)$ where α is an automorphism of G. Moreover, UVW is extensible in that it gives an automorphism of $\mathfrak{Q}(G, \Sigma)$. Furthermore, by Theorem 5 (ii), (iii), VW is extensible and thus $\rho(r)\Sigma\rho(s)^{-1} = \Sigma$. Therefore,

$$\alpha\Sigma\alpha^{-1} = \alpha[\rho(r)\ \Sigma\rho(s)^{-1}]\alpha^{-1} = [\alpha\rho(r)]\Sigma[\alpha\rho(s)]^{-1} = \Sigma,$$

showing that (α, α, α) is extensible and giving, by Theorem 5 (i), $\alpha\Delta\alpha^{-1} = \Delta$. But, even more, the translations, the automorphisms of $\mathfrak{Q}(G, \Sigma)$, and hence also the mappings $(x, y) \to (x\alpha, y\alpha)$ preserve parallel class. If we note the proof of Theorem 5 (i), we see that $\alpha^{-1}\delta\alpha = \delta$ for each $\delta \in \Delta$.

To prove the converse, suppose we have a mapping of $\mathfrak{Q}(G, \Sigma)$ as described in the statement of the theorem. The translations are automorphisms of $\mathfrak{N}(G)$ and the corresponding autotopism is a product of autotopisms of types (ii) and (iii):

$$(\rho(r), \rho(s - r), \rho(s)) = (\rho(r), \rho(r), \rho(r)^2)\ (\epsilon, \rho(s - 2r), \rho(s - 2r)).$$

Thus the translations correspond exactly to such products and, by Theorem 5 (ii), (iii), are extensible. In fact, they preserve parallel class. Also, by the proof of Theorem 5 (i), (α, α, α) is extensible and preserves parallel class in the extended net. Thus our mapping corresponds to the autotopism $(\alpha\rho(r), \alpha\rho(s - r), \alpha\rho(s))$ which is extensible and preserves parallel class and therefore gives an automorphism of $\mathfrak{Q}(G, \Sigma)$.

The translations $(x, y) \to (x + r, y + s)$ are transitive on the points of $\mathfrak{Q}(G, \Sigma)$ and we see that if $\mathfrak{Q}(G, \Sigma)$ is an affine plane, it is Veblen-Wedderburn **(8)**.

5. Linear adjoints and homomorphisms.

LEMMA 2. *Let G be a loop and $\sigma = \delta\rho(c)$ be a linear adjoint with companion $\gamma\rho(c)$. Then a normal subloop H of G is a σ-subloop if and only if $H\delta = H\gamma = H$.*

Proof. Assume $H\delta = H$. Then $x\delta + c = (y\delta + c) + h$ for $h \in H$ if and only if $x\delta + c = (y\delta + h') + c$ for $h' \in H$ if and only if $x\delta = y\delta + h'$. But $y\delta + h' = y\delta + h''\delta = (y + h'')\delta$ for $h'' \in H$. Thus $x\delta\rho(c) = y\delta\rho(c) + h$ if and only if $x = y + h''$. Similarly, $H\gamma = H$ implies $x \equiv y \bmod H$ if and only if $x\gamma\rho(c) \equiv y\gamma\rho(c) \bmod H$.

Now assume that H is a normal σ-subloop. Then $h \equiv 0 \bmod H$ if and only if $h\delta\rho(c) \equiv 0\delta\rho(c) \bmod H$ if and only if $h\delta + c \equiv c \bmod H$ if and only if $h\delta \equiv 0 \bmod H$; that is, $h \in H$ if and only if $h\delta \in H$. Similarly, $H\gamma = H$.

We remark that $H\delta \subseteq H$ if and only if $H\gamma \subseteq H$; for, if $h \in H$, $h\delta + c = h + (h\gamma + c) = (h' + h\gamma) + c$ for some $h' \in H$. Hence $h\delta = h' + h\gamma$ and thus

$h\delta \in H$ if and only if $h\gamma \in H$. Therefore, if G is an abelian group with descending chain condition or if G is a finite loop, we need only assume either $H\delta \subseteq H$ or $H\gamma \subseteq H$ in order to prove that a normal subloop H is a normal σ-subloop.

In any loop G, multiplication of mappings of G into G is left distributive over addition of mappings. If G has the inverse property, one readily verifies that the mappings of G into G form a loop (under addition) with the inverse property where $-\alpha$ is defined by $x(-\alpha) = -(x\alpha)$. Therefore, $-(\alpha + \beta) = (-\beta) + (-\alpha)$. Also, $-\alpha$ is one-one (onto) if and only if α is one-one (onto).

LEMMA 3. *Let G be a loop with the inverse property and let $\sigma_1 = \delta_1\rho(c_1)$ and $\sigma_2 = \delta_2\rho(c_2)$ be strongly linear adjoints on G where $\delta_1 - \delta_2$ is one-one on G. Then*

(i) *σ_1 and σ_2 are compatible,*

(ii) *if H is a normal $\{\sigma_1, \sigma_2\}$-subloop, the induced adjoints σ^*_1 and σ^*_2 are strongly linear on G/H. If $H \subseteq H(\delta_1 - \delta_2)$, then δ^*_1 and δ^*_2 are compatible.*

Proof. (i) Assume $x\delta_1 + c_1 = x\delta_2 + c_2$. Then $-(x\delta_2) + (x\delta_1 + c_1) = c_2$ and $-(x\delta_2) + x\delta_1 = x(-\delta_2 + \delta_1) = c_2 - c_1$. The solution is unique if $-\delta_2 + \delta_1$ is one-one. Since $\delta_1 - \delta_2$ is one-one so also is $-(\delta_1 - \delta_2) = \delta_2 - \delta_1$. Define the mapping θ on G by $x\theta = -x$. We see that θ is a permutation of G and that if α is an automorphism of G, then $\theta\alpha = -\alpha$. Therefore,

$$\theta(\delta_2 - \delta_1) = \theta\delta_2 + \theta(-\delta_1) = -\delta_2 + \theta(\theta\delta_1) = -\delta_2 + (\theta\theta)\delta_1 = -\delta_2 + \delta_1$$

is one-one. We note that if $\delta_1 - \delta_2$ is a permutation then $x\delta_1 + c_1 = x\delta_2 + c_2$ possesses a (unique) solution.

(ii) For $i = 1, 2$, $(x + H)\sigma^*_i = x\sigma_i + H = (x\delta_i + c_i) + H = (x\delta_i + H) + (c_i + H)$. Clearly, $c_i + H$ is in the associator of G/H and, by Lemma 2, $\delta^*_i : x + H \to x\delta_i + H$ is an automorphism of G/H. In the same way, the companion of σ^*_i is a strongly linear permutation and thus σ^*_i is a strongly linear adjoint.

Next, assume $(x + H)\delta^*_1 = (x + H)\delta^*_2$. Then, for some $h \in H$, $x\delta_1 = h + x\delta_2$ and thus $x\delta_1 - x\delta_2 = x(\delta_1 - \delta_2) = h = h'(\delta_1 - \delta_2)$ for some $h' \in H$. Since $\delta_1 - \delta_2$ is one-one, $x \in H$ and hence $0 + H$ is the unique solution of $X\delta^*_1 = X\delta^*_2$.

THEOREM 7. *Let G be an abelian group satisfying the descending chain condition. If Σ is a complete set of compatible linear adjoints and H is a Σ-subgroup, then the quasinets $\mathfrak{Q}(G, \Sigma)$ and $\mathfrak{Q}(G/H, \Sigma^*)$ are nets in the sense described in Theorem 6.*

Proof. Let Δ be the set of automorphisms in Σ and suppose δ_1 and δ_2 are distinct elements of Δ. Now $\delta_1 - \delta_2$ is an endomorphism of G and $x(\delta_1 - \delta_2) = 0$ implies $x\delta_1 = x\delta_2$. Since δ_1 and δ_2 are compatible and since $0\delta_1 = 0\delta_2$ we see that $x = 0$; that is, the kernel of $\delta_1 - \delta_2$ is 0 and $\delta_1 - \delta_2$ is one-one and has a right inverse. By the descending chain condition, $G(\delta_1 - \delta_2)^{r+1} = G(\delta_1 - \delta_2)^r$ for some r and thus $G(\delta_1 - \delta_2) = G$ showing, by Theorem 6, that $\mathfrak{Q}(G, \Sigma)$ is a net.

The set Σ^* of induced adjoints of G/H is certainly complete. Let δ^*_1 and δ^*_2 be distinct elements of Δ^*. Then $\delta^*_1 - \delta^*_2$ is an endomorphism of G/H and $(x + H)(\delta^*_1 - \delta^*_2) = H$ implies $(x + H)\delta^*_1 - (x + H)\delta^*_2 = (x\delta_1 - x\delta_2) + H = x(\delta_1 - \delta_2) + H = H$. Thus $x(\delta_1 - \delta_2) \in H$. But $H(\delta_1 - \delta_2) \subseteq H$ because H is a Σ-subgroup and, by the descending chain condition, there is an integer s such that $H(\delta_1 - \delta_2)^{s+1} = H(\delta_1 - \delta_2)^s$. As above, $H(\delta_1 - \delta_2) = H$ giving $x \in H$ and showing that $\delta^*_1 - \delta^*_2$ is an isomorphism. Since G/H satisfies the descending chain condition, $\mathfrak{Q}(G/H, \Sigma^*)$ is a net as before.

If Σ is a set of strongly linear adjoints on a loop G, we have seen that the set Δ of automorphisms in Σ plays a special role in identifying normal Σ-subloops and in questions of compatibility and extensibility. We shall focus attention now on Δ and the normal Δ-subloops, realizing that, for every $\delta \in \Delta$ and every a in the associator of G, there is an adjoint $\delta\rho(a)$ whose normal subloops are exactly the normal δ-subloops.

LEMMA 4. *Let G be a finite loop of order $n > 1$ and suppose Δ is a set of automorphism adjoints such that every pair in Δ is compatible. Then the number of elements in Δ is not more than $n - 2$.*

Proof. The lines $x = 0$, $y = 0$, and $y = x$ of $\mathfrak{N}(G)$ have exactly the point $(0, 0)$ in common. Further, $(0, 0)$ is the point shared by each of these three lines and the adjoined line determined by $\delta \in \Delta$. Moreover, by compatibility, every pair of adjoined lines shares exactly this point. Let d be the number of elements in Δ. $\mathfrak{N}(G)$ has n^2 points and we count the points on the above $d + 3$ lines:

$$(d + 3)(n - 1) + 1 \leqslant n^2.$$

Rejecting $n = 1$, we have $d \leqslant n - 2$.

Definition. A *compatible triple* (G, Δ, H) consists of a loop G with the inverse property, a set Δ of automorphism adjoints on G and a normal Δ-subloop H of G such that, for every distinct pair δ_1 and δ_2 in Δ, $\delta_1 - \delta_2$ is one-one on G and is a permutation on H. The *degree* of Δ (deg Δ) is the number of elements in Δ. $(G : H)$ denotes the index of H in G.

THEOREM 8. *If (G, Δ, H) is a compatible triple where Δ has finite degree, then either $(G : H) = 1$ or $(G : H) \geqslant \deg \Delta + 2$.*

Proof. Suppose $(G : H) > 1$. By Lemma 3 (ii), G/H is a loop with automorphism adjoints Δ^* and every pair δ^*_1, δ^*_2 from Δ^* is compatible. Moreover, deg Δ = deg Δ^* for suppose $(x + H)\delta^*_1 = (x + H)\delta^*_2$ for all x. Then, for each $x \in G$, there is an $h \in H$ such that $x\delta_1 = h + x\delta_2$ or $x(\delta_1 - \delta_2) = h$. But $\delta_1 - \delta_2$ is a permutation on H and hence $x \in H$, contradicting our assumption that $G \neq H$. If $(G : H)$ is finite, apply Lemma 4 to the loop G/H with adjoints Δ^* to obtain deg Δ = deg $\Delta^* \leqslant (G : H) - 2$.

COROLLARY 1. *If the inverse property loop G contains a characteristic normal subloop H of index 2 then G has no automorphism adjoints.*

Proof. If δ is an automorphism adjoint, take $\Delta = \delta$ so deg $\Delta = 1$. (G, Δ, H) is a compatible triple and thus $2 \geqslant 1 + 2$, a contradiction.

Example. The symmetric group on n symbols has no automorphism adjoints.

COROLLARY 2. *Let G be a finite loop with the inverse property and let E be a characteristic normal subloop of G. Then, if (G, Δ, H) is a compatible triple for any H,* deg $\Delta \leqslant (G : E) - 2$.

Proof. (G, Δ, E) is a compatible triple because E is a Δ-subloop since it is characteristic and, by finiteness, $\delta_1 - \delta_2$ is a permutation on E for every distinct pair from Δ.

6. Irreducible sets of linear adjoints.

Definition. Let G be a loop with a set Σ of adjoints. We say that Σ is *irreducible* if G has no proper normal Σ-subloops.

THEOREM 9. *Let G be a loop with a set Σ of adjoints so that the quasinet $\mathfrak{Q}(G, \Sigma)$ is an affine plane. Then Σ is irreducible.*

Proof. Given $x \neq 0$, $y \neq 0$, $x \neq y$ in G, there is a unique line of the plane through $(0, 0)$ and (x, y). If the line is in $\mathfrak{N}(G)$, either $x = 0$, $y = 0$, or $y = x$ but these are excluded. Therefore, there exists $\sigma \in \Sigma$ such that $0\sigma = 0$ and $x\sigma = y$. Now suppose H is a proper normal Σ-subloop of G. Choose $x = h \neq 0$ in H and $y \notin H$. Then $h \equiv 0 \bmod H$ implies $h\sigma \equiv 0\sigma = 0 \bmod H$ and thus $h\sigma = y$ is in H, a contradiction.

LEMMA 5. *Let G be a finite loop with an irreducible set Σ of strongly linear adjoints. Let Δ be the set of automorphisms belonging to the adjoints of Σ and let Ω be the centralizer of Δ in the semigroup of endomorphisms of G. Then the non-zero elements of Ω are automorphisms. If G is an abelian group, the finiteness restriction can be dropped.*

Proof. Let K be the kernel of $\omega \in \Omega$. Then $k \in K$, $\delta \in \Delta$ implies $(k\delta)\omega = (k\omega)\delta = 0\delta = 0$ and thus $K\delta \subseteq K$. But ω commutes also with δ^{-1} giving $K\delta = K$. Now $\epsilon + \gamma = \delta$ and since ω is an endomorphism, multiplication by ω is distributive on both sides over mapping addition. Thus, $\omega + \gamma\omega = \delta\omega$ and $\omega + \omega\gamma = \omega\delta$ showing $\omega\gamma = \gamma\omega$. As before, $K\gamma = K$. By Lemma 2 and irreducibility, $K = G$ or $K = 0$ and hence ω is the zero endomorphism or is one-one on G. In the latter case, since G is finite, ω is an automorphism. If G is an infinite abelian group, $G\omega = (G\delta)\omega = (G\omega)\delta$ and $G\omega = (G\gamma)\omega = (G\omega)\gamma$ showing that $G\omega$ is a (normal) Σ-subloop. Therefore, either $G\omega = 0$, in which case $G = 0$, or $G\omega = G$. In either case ω is an automorphism of G.

THEOREM 10. *Let G be a finite loop or an abelian group with an irreducible complete set Σ of strongly linear adjoints whose subset of automorphisms is Δ. Let Ω be the centralizer of Δ in the endomorphisms of G. Then the autotopism*

(ω, ω, ω) with $\omega \in \Omega$, ω not zero, is associated with an automorphism of $\mathfrak{N}(G)$ which leaves fixed every line in $\mathfrak{Q}(G, \Sigma)$ through the point $(0, 0)$. Conversely, every such automorphism of $\mathfrak{N}(G)$ is paired with an autotopism of the type described. Moreover, these autotopisms are extensible relative to Σ.

Proof. The automorphism associated with (ω, ω, ω) is $(x, y) \to (x\omega, y\omega)$. This obviously fixes the lines $x = 0$, $y = 0$, and $y = x$ of $\mathfrak{N}(G)$. If $\delta\rho(a) \in \Sigma$ determines an adjoined line through the origin, evidently $a = 0$ and $(x, x\delta) \to (x\omega, x\delta\omega) = (x\omega, (x\omega)\delta)$. Thus the line determined by δ maps into itself.

Conversely, let (α, γ, β) give an automorphism which fixes lines through $(0, 0)$. Then, in particular, $y = x$ is fixed and hence $(x, x) \to (x\alpha, x\beta)$ for all x implies $\alpha = \beta$. Therefore, $(x + y)\alpha = x\alpha + y\gamma$ for every x and y. Since $(0, 0)$ is fixed, $0\alpha = 0$ and we set $x = 0$ giving $y\alpha = y\gamma$. Therefore, the autotopism arises from an automorphism, $\alpha = \beta = \gamma$ of G. If $\delta \in \Delta$, the corresponding line is fixed and hence $(x, x\delta) \to (x\alpha, x\delta\alpha) = (x\alpha, (x\alpha)\delta)$ showing that α is in the centralizer of Δ.

Extensibility follows immediately and, in fact, if G and Σ satisfy the hypothesis of Theorem 6, α gives an automorphism of the quasinet $\mathfrak{Q}(G, \Sigma)$.

Suppose G is an abelian group and Σ, Δ, Ω are as in Theorem 10. Then Ω is a ring and, in fact, a division ring by Lemma 5. Therefore, we may regard G as a vector space over Ω and we note that the elements of Ω different from the zero and the identity are automorphism adjoints of G. If $\mathfrak{Q}(G, \Sigma)$ is a Veblen-Wedderburn plane as in Theorem 6, one may verify that Ω is André's "Kern" **(1)**.

7. A class of examples. The neofields of Paige **(7)** and their generalizations, the division neorings of Hughes **(5)**, provide a class of examples of loops with adjoints. If $(D, +, \cdot)$ is a division neoring (see **5** for definition), take G to be $(D, +)$ and define the mapping R_a on G by $xR_a = xa$ where $a \in D$. Clearly, R_a is a permutation for every $a \neq 0$. Then, every R_a with $a \neq 0, a \neq 1$ is an automorphism adjoint on G because $(x + y)R_c = xR_c + yR_c$ for every $c \in D$ and $x(e + R_b) = x + xb = x(1 + b) = xR_a$ where $b \neq 0$ is the unique solution of $1 + b = a$. If E is any subdivision neoring for which $(E, +)$ is normal in $(D, +)$, then $(E, +)$ is a normal Δ-subloop where Δ consists of the mappings R_e, $e \in E$, $e \neq 0$, $e \neq 1$. Moreover, if $(D, +)$ has the inverse property, then $((D, +), \Delta, (E, +))$ is a compatible triple.

References

1. Johannes André, *Ueber nicht-Desarguessche Ebenen mit transitiver Translationsgruppe*, Math. Zeitschr., *60* (1954), 156–186.
2. R. H. Bruck, *Contributions to the theory of loops*, Trans. Amer. Math. Soc., *60* (1946), 245–354.
3. ——— *Finite nets*, I. *Numerical invariants*, Can. J. Math., *3* (1951), 94–107.
4. Marshall Hall, *Projective planes*, Trans. Amer. Math. Soc., *54* (1943), 229–277.
5. D. R. Hughes, *Planar division neo-rings*, Trans. Amer. Math. Soc., *80* (1955), 502–527.
6. Henry B. Mann, *The construction of orthogonal Latin squares*, Ann. Math. Stat., *13* (1942), 418–423.
7. Lowell J. Paige, *Neofields*, Duke Math. J., *16* (1949), 39–60.
8. Günter Pickert, *Projektive Ebenen* (Berlin, 1955).

Montana State University

ON QUADRUPLE SYSTEMS

HAIM HANANI

1. Introduction. Given a set E of n elements we denote by $S(l, m, n)$, $(l \leqslant m \leqslant n)$ a system[1] of subsets of E, having m elements each, such that every subset of E having l elements is contained in exactly one set of the system $S(l, m, n)$.

It is clear **(3)**, that a necessary condition for the existence of $S(l, m, n)$ is that

$$\binom{n-h}{l-h} \Big/ \binom{m-h}{l-h} = \text{integer}, \qquad (h = 0, 1, \ldots, l-1). \tag{1}$$

$$\binom{n}{l} \Big/ \binom{m}{l}$$

is the number of elements of $S(l, m, n)$ and

$$\binom{n-h}{l-h} \Big/ \binom{m-h}{l-h}$$

is the number of those elements of $S(l, m, n)$ which contain h fixed elements of E.

It is known that condition (1) is not sufficient for $S(l, m, n)$ to exist. It has been proved that no finite projective geometry exists with 7 points on every line.[2] This implies non-existence of $S(2, 7, 43)$.

There arises a problem of finding a necessary and sufficient condition for the existence of $S(l, m, n)$, or more precisely, of finding—for given values of l and m—all values of n for which $S(l, m, n)$ exists.

Already in 1852 Steiner **(6)** (see also **(4)**) raised the following problem:

(a) For what integer N is it possible to form triples, out of N given elements, in such a way that every pair of elements appears in exactly one triple?

(b) Assuming (a) solved we require the further possibility of forming quadruples so that any three elements, not already forming a triple, should appear in exactly one quadruple and that no quadruple should contain a triple. Does this impose new conditions on the number N?

(c) Assuming (a) and (b) solved, can we moreover form quintuples so that any four elements, neither forming a quadruple nor containing a triple,

Received February 9, 1959.

[1]The term "family" would be more appropriate, but for historical reasons we shall use the term "system."

[2]This follows from the proof by G. Tarry that the "36 Offiziere" problem of Euler has no solution **(8)**.

should appear in exactly one quintuple and that no quintuple should contain a quadruple or a triple? Does this impose further restrictions on the number N?

Steiner carries on stating analogous problems for sixtuples, septuples, etc.

The problem of Steiner is essentially equivalent to that of $S(m-1, m, n)$ systems. The special case of $S(2, 3, n)$ constitutes Steiner's famous triple problem (a), and $S(3, 4, n)$ are equivalent to Steiner's quadruple problem (b) with $n = N + 1$. It can easily be seen that by adding an additional element to the system described in (b) and by joining it to every existing triple, a $S(3, 4, N+1)$ system evolves.

The present form of the problem is due to Moore **(3)**.

So far the problem has been solved completely only for $l = 2$, $m = 3$, that is, for triple systems: from (1) it follows that a necessary condition for the existence of $S(2, 3, n)$ is

$$n = 1 \quad \text{or} \quad 3 \pmod 6; \tag{2}$$

on the other hand, Reiss **(5)** and later independently Moore **(2)** proved that this condition is also sufficient. Other results are limited to special values of l, m, n. A list of systems $S(l, m, n)$ which are known to exist can be found in **(7)**.

In the case of $l = 3$, $m = 4$, that is, of quadruple systems, it follows from (1) that a necessary condition for the existence of $S(3, 4, n)$ is $n \equiv 2$ or $4 \pmod 6$. The object of the present paper is to prove that this condition is also sufficient.

2. Definitions and notation.

2.1. *The systems* $P_\alpha(m)$. Given a set of $2m$ elements $0, 1, \ldots, 2m-1$, we decompose the $m(2m-1)$ unordered pairs $[r, s]$ formed from them into $2m-1$ systems $P_\alpha(m)$, $(\alpha = 0, 1, \ldots, 2m-2)$, each containing m mutually disjoint pairs.[3]

For $m \equiv 0 \pmod 2$ we form the systems $P_\alpha(m)$ as follows:

$$P_{2\beta}(m) = \{[2a, 2a + 2\beta + 1] : a = 0, 1, \ldots, m-1\},$$

$$P_{2\beta+1}(m) = \{[2a, 2a - 2\beta - 1] : a = 0, 1, \ldots, m-1\},$$

$$(\beta = 0, 1, \ldots, \tfrac{1}{2}(m-2));$$

$$P_{m+\gamma}(m) = \left\{ \begin{array}{l} [b, 2\gamma - b] : b = 0, 1, \ldots, \gamma - 1 \\ [c, 2m + 2\gamma - c - 2] : c = 2\gamma + 1, 2\gamma + 2, \ldots, m + \gamma - 2 \\ \left[2m - \frac{3}{2} - (-1)^\gamma \tfrac{1}{2}, \gamma\right], \left[2m - \frac{3}{2} + (-1)^\gamma \tfrac{1}{2}, m + \gamma - 1\right] \end{array} \right\},$$

$$(\gamma = 0, 1, \ldots, m-2).$$

For $m \equiv 1 \pmod 2$ we put:

[3] Other systems of pairs may be found in **(5)** and **(4)**, but in the sequel we shall need the systems $P_\alpha(m)$ as defined here.

$$P_{2\beta}(m) = \{[2a, 2a + 2\beta + 1] : a = 0, 1, \ldots, m - 1\},$$
$$P_{2\beta+1}(m) = \{[2a, 2a - 2\beta - 1] : a = 0, 1, \ldots, m - 1\},$$
$$(\beta = 0, 1, \ldots, \tfrac{1}{2}(m - 3));$$

$$P_{m-1+\gamma}(m) = \left\{ \begin{matrix} [b, 2\gamma - b] : b = 0, 1, \ldots, \gamma - 1 \\ [c, 2m + 2\gamma - c] : c = 2\gamma + 1, 2\gamma + 2, \ldots, m + \gamma - 1 \\ [\gamma, m + \gamma] \end{matrix} \right\},$$
$$(\gamma = 0, 1, \ldots, m - 1).$$

It can be easily verified that the pairs in every system are mutually disjoint and that no pair appears twice. As the number of pairs in the systems is $m(2m - 1)$ it follows that every pair appears in some system.

2.2. *The systems* $\bar{P}_\xi(m)$. In the sequel we shall also need another decomposition of pairs formed from $2m$ elements, namely into $2m$ systems $\bar{P}_\xi(m)$, $(\xi = 0, 1, \ldots, 2m - 1)$ such that each of the m systems $\bar{P}_\eta(m)$, $(\eta = 0, 1, \ldots, m - 1)$ should contain $m - 1$ mutually disjoint pairs not containing the elements 2η and $2\eta + 1$, and each of the other m systems should contain m mutually disjoint pairs.

We shall form the systems $\bar{P}_\xi(m)$ using the systems $P_\alpha(m)$ defined in the preceding section.

If $m \equiv 0 \pmod 2$ it can easily be seen that

$$[2\mu, 4\mu + 1] \in P_{2\mu}(m),$$
$$[2m - 2 - 2\mu, 2m - 1 - 4\mu] \in P_{2\mu-1}(m), \quad (\mu = 1, 2, \ldots, \tfrac{1}{2}(m - 2));$$
$$[2m - 2, 0] \in P_m(m); \quad [2m - 1, 1] \in P_{m+1}(m).$$

Clearly, these pairs are mutually disjoint. We remove them from their respective systems and form from them a new system.

Performing the following permutation of the elements

$$\begin{pmatrix} 2\mu, 4\mu + 1, 2m - 2 - 2\mu, 2m - 1 - 4\mu, 2m - 2, 0, 2m - 1, 1 \\ 4\mu, 4\mu + 1, 4\mu - 2 \quad , 4\mu - 1 \quad , 1 \quad , 0, 2m - 1, 2m - 2 \end{pmatrix}$$
$$(\mu = 1, 2, \ldots, \tfrac{1}{2}(m - 2))$$

we obtain by a suitable reordering of the systems the new systems $\bar{P}_\xi(m)$.

In the case $m \equiv 1 \pmod 2$ we have

$$[2\mu, 4\mu + 1] \in P_{2\mu}(m),$$
$$[2m - 2 - 2\mu, 2m - 3 - 4\mu] \in P_{2\mu+1}(m), \quad (\mu = 0, 1, \ldots, \tfrac{1}{2}(m - 3));$$
$$[m - 1, 2m - 1] \in P_{2m-2}(m).$$

These pairs are again mutually disjoint.

By the permutation

$$\begin{pmatrix} 2\mu, 4\mu + 1, 2m - 2 - 2\mu, 2m - 3 - 4\mu, m - 1 \ , 2m - 1 \\ 4\mu, 4\mu + 1, 4\mu + 2 \quad , 4\mu + 3 \quad , 2m - 2, 2m - 1 \end{pmatrix},$$
$$(\mu = 0, 1, \ldots, \tfrac{1}{2}(m - 3)),$$

of the elements and using the same procedure as in the case $m \equiv 0 \pmod 2$ we obtain the systems $P_t(m)$.

2.3. *The quadruples.* Let there be given a set F of f elements $0, 1, \ldots, f-1$. If a system $S(3, 4, f)$ exists we say that it is possible to form a quadruple system from F and we write $F \in Q$ and also $f \in Q$.

If $F \in Q$, we shall in the sequel denote by $\{x, y, z, t\} \subset F$ any quadruple in F, that is, an element of $S(3, 4, f)$. The number of quadruples will be denoted by $q(f)$:

$$q(f) = \frac{1}{24} f(f-1)(f-2).$$

If $f + 1 \in Q$, then $F \cup \{A\} \in Q$ where A is some additional element. The quadruples which contain A will be denoted by $\{A, u, v, w\}$ and their number by $p(f)$:

$$p(f) = \frac{1}{6} f(f-1).$$

The other quadruples will be denoted by $\{x, y, z, t\}$ and their number by $q'(f)$:

$$q'(f) = q(f+1) - p(f) = \frac{1}{24} f(f-1)(f-3).$$

2.4. *The elements.* Elements of the sets used in this paper will often be denoted by a pair of numbers (i, j), $(i = 0, 1, \ldots, g-1; j = 0, 1, \ldots, f-1)$ i will then be called the first index and j the second index of the element.

For the sake of uniformity we shall denote sometimes elements by (A, h), $(h = 0, 1, \ldots, e-1)$ instead of the more commonly used notation A_h.

In the above notation we shall also include elements (a, b), (A, c) with a, b, and c not necessarily restricted to $a < g$, $b < f$, and $c < e$. In these cases the indices are to be taken modulo g, f, and e respectively.

2.5. *Checking of systems.* In order to show that some given family of quadruples formed from the elements of a set N (having n elements) are a system it must be proved that:

(i) Every subset of N having 3 elements is contained in some quadruple.

(ii) The intersection of every two quadruples has 2 elements at most.

Evidently (i) will imply (ii) if it can be verified that the total number of the quadruples is $q(n)$ and we shall use this method of checking the systems in the sequel.

3. THEOREM. *A system $S(3, 4, n)$ exists if and only if $n \equiv 2$ or $4 \pmod 6$.*

Proof. The necessity has been proved in § 1. The proof of sufficiency will be given by induction. Evidently $4 \in Q$. We shall show that if $n \equiv 2$ or $4 \pmod 6$ and if for every $g < n$ satisfying $g \equiv 2$ or $4 \pmod 6$, $g \in Q$ holds, then also $n \in Q$. The proof will be given separately for each of the following cases which evidently exhaust all the possibilities:

3.1. $n \equiv 4$ or $8 \pmod{12}$,

3.2. $n \equiv 4$ or $10 \pmod{18}$,

3.3. $n \equiv 34 \pmod{36}$,

3.4. $n \equiv 26 \pmod{36}$,

3.5. $n \equiv 2$ or $10 \pmod{24}$, $(n > 2)$,

3.6. $n \equiv 14$ or $38 \pmod{72}$.

3.1.[4] $n \equiv 4$ or $8 \pmod{12}$. We put $n = 2f$, where $f \equiv 2$ or $4 \pmod 6$ and by the assumption of the induction $f \in Q$. Denote $F = \{j : j = 0, 1, \ldots, f-1\}$, $N = \{(i, j) : i = 0, 1; j = 0, 1, \ldots, f-1\}$. Further let $\{x, y, z, t\}$ be any quadruple in F; the number of such quadruples is $q(f)$.

Form the following quadruples in N:

$L_1 : (a_1, x)(a_2, y)(a_3, z)(a_4, t)$, $a_1 + a_2 + a_3 + a_4 \equiv 0 \pmod 2$;

$L_2 : (0, j)(0, j')(1, j)(1, j')$, $(j = 0, 1, \ldots, f-1; j' = 0, 1, \ldots, f-1; j \neq j')$

In the quadruples L_1 three of the indices a_1, a_2, a_3, a_4 can be chosen freely from the numbers 0 and 1, and accordingly the number of these quadruples is $8q(f)$. The number of quadruples L_2 is evidently $\frac{1}{2}f(f-1)$. The total number of quadruples is therefore $8q(f) + \frac{1}{2}f(f-1) = q(n)$.

By 2.5, it remains to be shown that every subset of N containing 3 elements $\{(i_1, j_1)(i_2, j_2)(i_3, j_3)\}$ is included in some quadruple. This is, however, evident as:

(a) if $j_1 \neq j_2 \neq j_3 \neq j_1$ it is included in some L_1;

(b) otherwise it is included in some L_2.

Consequently $n \in Q$.

3.2. $n \equiv 4$ or $10 \pmod{18}$. Put $n = 3f + 1$, where $f = 1$ or $3 \pmod 6$. Thus $f + 1 \in Q$. Denote $F = \{j : j = 0, 1, \ldots, f-1\}$, $N = \{(A); (i, j) : i = 0, 1, 2; j = 0, 1, \ldots, f-1\}$. (See 2.3 for definitions of $\{(A), u, v, w\}$ and $\{x, y, z, t\}$.)

Form the following quadruples in N: their number being:

$L_1 : (a_1, x)(a_2, y)(a_3, z)(a_4, t)$, $a_1 + a_2 + a_3 + a_4 \equiv 0 \pmod 3$;	$27q'(f)$
$L_2 : (A)(b_1, u)(b_2, v)(b_3, w)$, $b_1 + b_2 + b_3 \equiv 0 \pmod 3$;	$9p(f)$
$L_3 : (i, u)(i, v)(i+1, w)(i+2, w)$,	$9p(f)$
$L_4 : (i, j)(i, j')(i+1, j)(i+1, j')$, $j \neq j'$;	$3 \cdot \frac{1}{2}f(f-1)$
$L_5 : (A)(0, j)(1, j)(2, j)$;	f
totalling	$q(n)$.

[4] This part of the proof is not new. It is well known that from $f \in Q$ follows $2f \in Q$, (see, for example, **(1)** and **(7)**).

Now every subset T of N containing three elements is contained in one of the quadruples, namely:

(a) if $T = \{(A)(i_1, j_1)(i_2, j_2)\}$ and

(aa) if $j_1 \neq j_2$, in some L_2;

(ab) if $j_1 = j_2$, in some L_5;

(b) if $T = \{(i_1, j_1)(i_2, j_2)(i_3, j_3)\}$ and

(ba) if $j_1 \neq j_2 \neq j_3 \neq j_1$ and

(baa) if j_1, j_2, j_3 form a $\{u, v, w\}$, in L_2 or in L_3;

(bab) otherwise, in L_1;

(bb) if $j_1 = j_2 \neq j_3$ and

(bba) if $i_1 \neq i_2 \neq i_3 \neq i_1$, in L_3;

(bbb) otherwise, in L_4

(bc) if $j_1 = j_2 = j_3$, in L_5.

It is thus proved that $n \in Q$.

3.3. $n = 34 \pmod{36}$. Put $n = 3f + 4$, where $f \equiv 10 \pmod{12}$ and denote $f = 12k + 10$. Here $f + 4 \in Q$. Denote $F = \{j : j = 0, 1, \ldots, f - 1\}$, $N = \{(i, j); (A, h) : i = 0, 1, 2; j = 0, 1, \ldots, f - 1; h = 0, 1, 2, 3\}$. We have $\bar{F} = F \cup \{(A, h) : h = 0, 1, 2, 3\} \in Q$. By $\{x, y, z, t\}$ we denote quadruples in $\bar{F}$, one of them being $\{(A, h) : h = 0, 1, 2, 3\}$.

Form the following quadruples in N: their number being:

$L_1 : (A, 0)(A, 1)(A, 2)(A, 3)$; 1

$L_2 : (i, x)(i, y)(i, z)(i, t)$,[5] $3[q(f + 4) - 1]$
quadruple L_1 excluded;

$L_3 : (A, a_1)(0, a_2)(1, a_3)(2, a_4)$, $4f^2$
$a_1 + a_2 + a_3 + a_4 \equiv 0 \pmod{f}$;

$L_4 : (i + 2, b_3)(i, b_1 + 2k + 1 + i(4k + 2) - d)(i, b_1 + 2k + 2 + i(4k + 2) + d)(i + 1, b_2)$, $3(2k + 1)f^2$
$b_1 + b_2 + b_3 \equiv 0 \pmod{f}$,
$d = 0, 1, \ldots, 2k$;

$L_5 : (i, r_\alpha)(i, s_\alpha)(i + 1, r_\alpha')(i + 1, s_\alpha')$, $3(8k + 7)(\frac{1}{2}f)^2$
$[r_\alpha, s_\alpha]$ and $[r_\alpha', s_\alpha']$ are (equal or different) pairs in $P_\alpha(6k + 5)$, (see 2.1.),
$\alpha = 4k + 2, 4k + 3, \ldots, 12k + 8$;

totalling $q(n)$

[5] Whenever for x, y, z, or t appears (A, h), omit the first index i.

Again, every subset T of N containing three elements is contained in some quadruple:

(a) if $T = \{(A, h_1)(A, h_2)(A, h_3)\}$, in L_1;
(b) if $T = \{(A, h_1)(A, h_2)(i_1, j_1)\}$, in L_2;
(c) if $T = \{(A, h_1)(i_1, j_1)(i_2, j_2)$ and
  (ca) if $i_1 = i_2$, in L_2;
  (cb) otherwise, in L_3;
(d) if $T = \{(i_1, j_1)(i_2, j_2)(i_3, j_3)\}$ and
  (da) if $i_1 \neq i_2 \neq i_3 \neq i_1$ and
    (daa) if $j_1 + j_2 + j_3 \equiv f - 3, f - 2, f - 1$, or $0 \pmod f$, in L_3;
    (dab) otherwise, in L_4;
  (db) if $i_1 = i_2 \neq i_3$ and
    (dba) if $|j_2 - j_1| \equiv 1 \pmod 2$ and $|j_2 - j_1| < 4k + 1$, in L_4;
    (dbb) otherwise, in L_5;
  (dc) if $i_1 = i_2 = i_3$, in L_2.

Thus $n \in Q$.

3.4. $n \equiv 26 \pmod{36}$. Here $n = 3f + 2$, $f \equiv 8 \pmod{12}$, or $f = 12k + 8$; $f + 2 \in Q$. Denote $F = \{j : j = 0, 1, \ldots, f - 1\}$, $N = \{(i, j); (A, h) : i = 0, 1, 2; j = 0, 1, \ldots, f - 1; h = 0, 1\}$. We have $\bar{F} = F \cup \{(A, h) : h = 0, 1\} \in Q$. By $\{x, y, z, t\}$ denote quadruples in $\bar{F}$.

Form the following quadruples in N: their number being:

$L_2 : (i, x)(i, y)(i, z)(i, t)$;[6] $3q(f + 2)$

$L_3 : (A, a_1)(0, a_2)(1, a_3)(2, a_4)$, $2f^2$
$a_1 + a_2 + a_3 + a_4 \equiv 0 \pmod f$;

$L_4 : (i + 2, b_3)(i, b_1 + 2k + 1 + i(4k + 2) - d)(i, b_1 + 2k + 2 + i(4k + 2) + d)(i + 1, b_2)$, $3(2k + 1)f^2$
$b_1 + b_2 + b_3 \equiv 0 \pmod f$,
$d = 0, 1, \ldots, 2k$;

$L_5 : (i, r_\alpha)(i, s_\alpha)(i + 1, r_\alpha')(i + 1, s_\alpha')$, $3(8k + 5)(\frac{1}{2}f)^2$
$[r_\alpha, s_\alpha]$ and $[r_\alpha', s_\alpha']$ are pairs in $P_\alpha(6k + 4)$,
$\alpha = 4k + 2, 4k + 3, \ldots, 12k + 6$;

totalling $q(n)$

Checking that every subset of N containing 3 elements is contained in some quadruple is made in the same way as in the preceding section with the only difference that: the case (a) is omitted and (daa) reads: if $j_1 + j_2 + j_3 \equiv f - 1$, or $0 \pmod f$ a.s.o. Consequently $n \in Q$.

[6] *Ibid.*

3.5. $n \equiv 2$ or $10 (\mathrm{mod}\ 24)$, $n > 2$. Put $n = 4f + 2$, $f \equiv 0$ or $2 (\mathrm{mod}\ 6)$, $(f > 0)$; $f = 2k$; by the assumption of the induction $f + 2 \in Q$. Denote $F = \{j : j = 0, 1, \ldots, f - 1\}$, $N = \{(h, i, j); (A, l) : h = 0, 1; i = 0, 1; j = 0, 1, \ldots, f - 1; l = 0, 1\}$. By $\{x, y, z, t\}$ denote quadruples in $F \cup \{(A, l): l = 0, 1\} \in Q$.

Form the quadruples in N: their number being:

$L_1 : (h, i, x)(h, i, y)(h, i, z)(h, i, t)$;[7] $4q(f + 2)$

$L_2 : (A, l)(0, 0, 2c_1)(0, 1, 2c_2 - \epsilon)(1, \epsilon, 2c_3 + l)$, f^2
$c_1 + c_2 + c_3 \equiv 0 (\mathrm{mod}\ k)$,
$\epsilon = 0, 1$;

$L_3 : (A, l)(0, 0, 2c_1 + 1)(0, 1, 2c_2 - 1 - \epsilon)(1, \epsilon, 2c_3 + 1 - l)$; f^2

$L_4 : (A, l)(1, 0, 2c_1)(1, 1, 2c_2 - \epsilon)(0, \epsilon, 2c_3 + 1 - l)$; f^2

$L_5 : (A, l)(1, 0, 2c_1 + 1)(1, 1, 2c_2 - 1 - \epsilon)(0, \epsilon, 2c_3 + l)$; f^2

$L_6 : (h, 0, 2c_1 + \epsilon)(h, 1, 2c_2 - \epsilon)(h + 1, 0, \bar{r}_{c_3})(h + 1, 0, \bar{s}_{c_3})$, $(k - 1)f^2$
$[\bar{r}_{c_3}, \bar{s}_{c_3}]$ are pairs in $\bar{P}_{c_3}(k)$, (see 2.2),
$c_3 = 0, 1, \ldots, k - 1$;

$L_7 : (h, 0, 2c_1 - 1 + \epsilon)(h, 1, 2c_2 - \epsilon)(h + 1, 1, \bar{r}_{c_3})(h + 1, 1, \bar{s}_{c_3})$; $(k - 1)f^2$

$L_8 : (h, 0, 2c_1 + \epsilon)(h, 1, 2c_2 - \epsilon)(h + 1, 1, \bar{r}_{k+c_3})(h + 1, 1, \bar{s}_{k+c_3})$; kf^2

$L_9 : (h, 0, 2c_1 - 1 + \epsilon)(h, 1, 2c_2 - \epsilon)(h + 1, 0, \bar{r}_{k+c_3})(h + 1, 0, \bar{s}_{k+c_3})$; kf^2

$L_{10} : (h, 0, r_\alpha)(h, 0, s_\alpha)(h, 1, r_\alpha')(h, 1, s_\alpha')$, $2(f - 1)k^2$
$[r_\alpha, s_\alpha]$ and $[r_\alpha', s_\alpha']$ are pairs
in $P_\alpha(k)$, (see 2.1.),
$\alpha = 0, 1, \ldots, f - 2$;

totalling $q(n)$

It will now be checked that every triple T in N is contained in some quadruple.

(a) If T is of the form $\{(A, 0)(A, 1)(h_1, i_1, j_1)\}$, it is contained in some L_1;

(b) if $T = \{(A, l_1)(h_1, i_1, j_1)(h_2, i_2, j_2)\}$ and

(ba) if $h_1 = h_2$ and

(baa) if $i_1 = i_2$, in L_1;

(bab) if $i_1 \neq i_2$ say $i_1 = 0$, $i_2 = 1$ and

(baba) if $j_1 \equiv 0 (\mathrm{mod}\ 2)$, in L_2 or L_4;

(babb) if $j_1 \equiv 1 (\mathrm{mod}\ 2)$, in L_3 or L_5;

[7] *Ibid.*

(bb) if $h_1 \neq h_2$ say $h_1 = 0$, $h_2 = 1$ and
  (bba) if $i_1 = i_2 = 0$ and
    (bbaa) if $j_1 + j_2 + l_1 \equiv 0 \pmod 2$, in L_2 or L_3, $(\epsilon = 0)$;
    (bbab) if $j_1 + j_2 + l_1 \equiv 1 \pmod 2$, in L_4 or L_5, $(\epsilon = 0)$;
  (bbb) if $i_1 = i_2 = 1$ and
    (bbba) if $j_1 + j_2 + l_1 \equiv 0 \pmod 2$, in L_4 or L_5, $(\epsilon = 1)$;
    (bbbb) if $j_1 + j_2 + l_1 \equiv 1 \pmod 2$, in L_2 or L_3, $(\epsilon = 1)$;
  (bbc) if $i_1 = 0$, $i_2 = 1$, and
    (bbca) if $j_1 + j_2 + l_1 \equiv 0 \pmod 2$, in L_2 or L_3, $(\epsilon = 1)$;
    (bbcb) if $j_1 + j_2 + l_1 \equiv 1 \pmod 2$, in L_4 or L_5, $(\epsilon = 0)$;
  (bbd) if $i_1 = 1$, $i_2 = 0$ and
    (bbda) if $j_1 + j_2 + l_1 \equiv 0 \pmod 2$, in L_2 or L_3, $(\epsilon = 0)$;
    (bbdb) if $j_1 + j_2 + l_1 \equiv 1 \pmod 2$, in L_4 or L_5, $(\epsilon = 1)$;

(c) if $T = \{(h_1, i_1, j_1)(h_2, i_2, j_2)(h_3, i_3, j_3)\}$ and
  (ca) if $h_1 = h_2 = h_3$ and
    (caa) if $i_1 = i_2 = i_3$, in L_1;
    (cab) otherwise, in L_{10};
  (cb) if $h_1 = h_2 \neq h_3$ and
    (cba) if $i_1 = i_2 = 0$, in L_8 or L_9;
    (cbb) if $i_1 = i_2 = 1$, in L_7 or L_8;
    (cbc) if $i_1 \neq i_2$, say $i_1 = 0$, $i_2 = 1$ and
      (cbca) if $i_3 = 0$ and
        (cbcaa) if $j_1 + j_2 \equiv 1 \pmod 2$, in L_9;
        (cbcab) if $j_1 + j_2 \equiv 0 \pmod 2$ and
          (cbcaba) if $j_1 + j_2 + j_3 \not\equiv 0, 1 \pmod f$, in L_6;
          (cbcabb) if $j_1 + j_2 + j_3 \equiv 0$ or $1 \pmod f$, then
            if $h_1 = h_2 = 0$, in L_2 or L_3, $(\epsilon = 0)$;
            if $h_1 = h_2 = 1$, in L_4 or L_5, $(\epsilon = 0)$;
      (cbcb) if $i_3 = 1$ and
        (cbcba) if $j_1 + j_2 \equiv 0 \pmod 2$, in L_8;
        (cbcbb) if $j_1 + j_2 \equiv 1 \pmod 2$ and
          (cbcbba) if $j_1 + j_2 + j_3 \not\equiv 0, f - 1 \pmod f$, in L_7;
          (cbcbbb) if $j_1 + j_2 + j_3 \equiv 0$ or $f - 1 \pmod f$, then
            if $h_1 = h_2 = 0$, in L_2 or L_3, $(\epsilon = 1)$;
            if $h_1 = h_2 = 1$, in L_4 or L_5, $(\epsilon = 1)$.

This proves that $n \in Q$.

3.6. $n \equiv 14$ or $38 \pmod{72}$. Here $n = 12f + 2$, $f \equiv 1$ or $3 \pmod 6$ and $f + 1 \in Q$. We shall prove that $n \in Q$.

We begin proving that $14 \in Q$. We take as elements the 14 symbols:

$$0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D;$$

and form $q(14) = 91$ quadruples as follows:

0125	038D	1236	157C	24AC	3579	479C
013B	039A	1247	1589	24BD	358B	5678
0146	0459	128B	15BD	257B	35AC	569B
0178	047B	129A	1679	258A	367B	56CD
019D	048A	12CD	168D	259C	3689	59AD
01AC	04CD	1345	16BC	267C	36AD	68AC
0234	057D	137D	17AB	269D	3BCD	789A
0268	058C	138A	235D	26AB	457A	78BC
0279	05AB	139C	237A	278D	458D	79BD
02AD	067A	148C	238C	346C	45BC	7ACD
02BC	069C	149B	239B	3478	467D	89CD
0356	06BD	14AD	2456	349D	468B	8ABD
037C	089B	156A	2489	34AB	469A	9ABC

It can be easily checked that every three elements are included in some quadruple and consequently these quadruples form a $S(3, 4, 14)$.

We now form the set $N' = \{(i, j); (A, h) : i = 0, 1, 2; j = 0, 1, \ldots, 11; h = 0, 1\}$ having 38 elements and we will show that $N' \in Q$. The system of quadruples in N' will be constructed so that it will contain all the quadruples in $\{(i, j); (A, h); j = 0, 1, \ldots, 11; h = 0, 1\}$ for $i = 0, 1, 2$. By $\{x', y', z', t'\}$ denote quadruples in $\{j; (A, h): j = 0, 1, \ldots, 11; h = 0, 1\}$.

Form the following quadruples: their number being:

$L_1 : (i, x')(i, y')(i, z')(i, t')$;[8] 273

$L_2 : (A, h)(0, b_1)(1, b_2)(2, b_3 + 3h)$, 288
$b_1 + b_2 + b_3 \equiv 0 \pmod{12}$,
$h = 0, 1$;

$L_3 : (i, b_1 + 4 + i)(i, b_1 + 7 + i)(i + 1, b_2)(i + 2, b_3)$; 432

$L_4 : (i, j)(i + 1, j + 6\epsilon)(i + 2, 6\epsilon - 2j + 1)(i + 2, 6\epsilon - 2j - 1)$, 72
$\epsilon = 0, 1$;

$L_5 : (i, j)(i + 1, j + 6\epsilon)(i + 2, 6\epsilon - 2j + 2)(i + 2, 6\epsilon - 2j - 2)$; 72

$L_6 : (i, j)(i + 1, j + 6\epsilon - 3)(i + 2, 6\epsilon - 2j + 1)(i + 2, 6\epsilon - 2j + 2)$; 72

$L_7 : (i, j)(i + 1, j + 6\epsilon + 3)(i + 2, 6\epsilon - 2j - 1)(i + 2, 6\epsilon - 2j - 2)$; 72

$L_8 : (i, j)(i, j + 6)(i + 1, j + 3\epsilon)(i + 1, j + 6 + 3\epsilon)$; 36

[8] *Ibid.*

$L_9 : (i, 2g + 3\epsilon)(i, 2g + 6 + 3\epsilon)(i', 2g + 1)(i', 2g + 5)$, 72
$i' \neq i$,
$g = 0, 1, 2, 3, 4, 5$;

$L_{10} : (i, 2g + 3\epsilon)(i, 2g + 6 + 3\epsilon)(i', 2g + 2)(i', 2g + 4)$; 72

$L_{11} : (i, j)(i, j + 1)(i + 1, j + 3e)(i + 1, j + 3e + 1)$, 144
$e = 0, 1, 2, 3$;

$L_{12} : (i, j)(i, j + 2)(i + 1, j + 3e)(i + 1, j + 3e + 2)$; 144

$L_{13} : (i, j)(i, j + 4)(i + 1, j + 3e)(i + 1, j + 3e + 4)$; 144

$L_{14} : (i, r_\alpha)(i, s_\alpha)(i', r_\alpha')(i', s_\alpha')$ 216
$[r_\alpha, s_\alpha]$ and $[r_\alpha', s_\alpha']$ are pairs
in $P_\alpha(6)$, (see 2.1),
$\alpha = 4, 5$;

totalling $2109 = q(38)$

Checking that every triple T' in N' is contained in some quadruple is carried out as follows:

(a) if $T' = \{(A, 0)(A, 1)(i_1, j_1)\}$, it is contained in L_1;

(b) if $T' = \{(A, h_1)(i_1, j_1)(i_2, j_2)\}$ and
  (ba) if $i_1 = i_2$, in L_1;
  (bb) if $i_1 \neq i_2$, in L_2;

(c) if $T' = \{(i_1, j_1)(i_2, j_2)(i_3, j_3)\}$ and
  (ca) if $i_1 = i_2 = i_3$, in L_1;
  (cb) if $i_1 = i_2 \neq i_3$, we may assume that $1 \leqslant (j_2 - j_1) \pmod{12} \leqslant 6$.
  Now
    (cba) if $j_1 + j_2 + j_3 \not\equiv 0 \pmod 3$ and
      (cbaa) if $j_2 - j_1 \equiv 1 \pmod{12}$, in L_{11};
      (cbab) if $j_2 - j_1 \equiv 2 \pmod{12}$, in L_{12};
      (cbac) if $j_2 - j_1 \equiv 3 \pmod{12}$, in L_3;
      (cbad) if $j_2 - j_1 \equiv 4 \pmod{12}$, in L_{13};
      (cbae) if $j_2 - j_1 \equiv 5 \pmod{12}$, in L_{14};
      (cbaf) if $j_2 - j_1 \equiv 6 \pmod{12}$, in L_9 or L_{10};
    (cbb) if $j_1 + j_2 + j_3 \equiv 0 \pmod 3$ and
      (cbba) if $j_2 - j_1 \equiv 1 \pmod{12}$ and
        (cbbaa) if $j_1 \equiv 0 \pmod 2$, in L_7;
        (cbbab) if $j_1 \equiv 1 \pmod 2$ in L_8;
      (cbbb) if $j_2 - j_1 \equiv 2 \pmod{12}$ and
        (cbbba) if $j_1 \equiv 0 \pmod 2$, in L_{10};
        (cbbbb) if $j_1 \equiv 1 \pmod 2$, in L_4;

(cbbc) if $j_2 - j_1 \equiv 3 \pmod{12}$, in L_3;
(cbbd) if $j_2 - j_1 \equiv 4 \pmod{12}$ and
(cbbda) if $j_1 \equiv 0 \pmod 2$, in L_8;
(cbbdb) if $j_1 \equiv 1 \pmod 2$, in L_9;
(cbbe) if $j_2 - j_1 \equiv 5 \pmod{12}$, in L_{14};
(cbbf) if $j_2 - j_1 \equiv 6 \pmod{12}$, in L_8;

(cc) if $i_1 \neq i_2 \neq i_3 \neq i_1$ and
(cca) if $j_1 + j_2 + j_3 \equiv 0$ or $3 \pmod{12}$, in L_2;
(ccb) if $j_1 + j_2 + j_3 \equiv 4, 5, 6, 7, 8$, or $9 \pmod{12}$, in L_3;
(ccc) if $j_1 + j_2 + j_3 \equiv 1, 2, 10$ or $11 \pmod{12}$ it is evident that two of the second indices, say j_1 and j_2 must be $j_2 - j_1 \equiv 0 \pmod 3$. Now
(ccca) if $j_2 - j_1 \equiv 0 \pmod 6$ and
(cccaa) if $j_1+j_2+j_3 \equiv 1$ or $11 \pmod{12}$, T' is contained in L_4;
(cccab) if $j_1 + j_2 + j_3 \equiv 2$ or $10 \pmod{12}$, in L_5;
(cccb) if $j_2 - j_1 \equiv 3 \pmod 6$ and
(cccba) if $j_1 + j_2 + j_3 \equiv 1$ or $2 \pmod{12}$, in L_7;
(cccbb) if $j_1 + j_2 + j_3 \equiv 10$ or $11 \pmod{12}$, in L_6.

Thus $38 \in Q$ is proved.

We are now able to prove the case $n \equiv 14$ or $38 \pmod{72}$, (that is, $f \equiv 1$ or $3 \pmod 6$) generally. We introduce an auxiliary element B and obtain $\bar{F} = \{j; B: j = 0, 1, \ldots, f-1\} \in Q$. (The quadruples $\{B, u, v, w\}$ and $\{x, y, z, t\}$ in $\bar{F}$ are defined in § 2.3.) Denote $N = \{(i, j); (A, h): i = 0, 1, \ldots, f-1; j = 0, 1, \ldots, 11; h = 0, 1\}$ and form the quadruples in N:

their number being:

$M_1 : (i, x')(i, y')(i, z')(i, t')$;[9] $91.f$

$$M_2 : \begin{cases} (A, h)(u, b_1)(v, b_2)(w, b_3 + 3h), \\ \qquad\qquad b_1 + b_2 + b_3 \equiv 0 \pmod{12}; \\ (u, \alpha_1)(v, \alpha_2)(w, \alpha_3)(w, \alpha_4); \\ (i, \beta_1)(i, \beta_2)(i', \beta_3)(i', \beta_4) \\ \qquad\qquad i' \neq i. \end{cases} \qquad (2109\text{-}273) \cdot p(f)$$

α_ν, β_ν, $(\nu = 1, 2, 3, 4)$ are to be replaced by the second indices of $L_2 - L_{14}$ corresponding to the first indices 0, 1, 2 for u, v, w respectively. It should be noted that i and i' define uniquely a $\{u, v, w\}$ in which they are contained and therefore they may be considered as two indices from this $\{u, v, w\}$.

$M_3 : (x, a_1)(y, a_2)(z, a_3)(t, a_4), a_1 + a_2 + a_3 + a_4 \equiv 0 \pmod{12}$; $1728.q'(f)$

totalling $q(n)$

[9] *Ibid.*

It is easy to see that every triple T in N is contained in some quadruple:

(a) if $T = \{(A,0)(A,1)(i_1,j_1)\}$ it is contained in M_1;

(b) if $T = \{(A,h_1)(i_1,j_1)(i_2,j_2)\}$ and
  (ba) if $i_1 = i_2$, it is contained in M_1;
  (bb) if $i_1 \neq i_2$, in M_2;

(c) if $T = \{(i_1,j_1)(i_2,j_2)(i_3,j_3)\}$ and
  (ca) if $i_1 = i_2 = i_3$, in M_1;
  (cb) if $i_1 = i_2 \neq i_3$, in M_2;
  (cc) if $i_1 \neq i_2 \neq i_3 \neq i_1$, and
    (cca) if i_1, i_2, i_3 form a $\{u,v,w\}$, in M_3;
    (ccb) otherwise in M_3.

Consequently in this case again $n \in Q$, and the proof is herewith completed.

References

1. R. D. Carmichael, *Introduction to the theory of groups of finite order* (New York, 1956), 415–441.
2. E. H. Moore, *Concerning triple systems*, Math. Annal. *43* (1893), 271–285.
3. ——— *Tactical memoranda*, Amer. J. Math. *18* (1896), 264–303.
4. E. Netto, *Lehrbuch der Combinatorik*, zweite Auflage (Leipzig, 1927), pp. 202–220, 321–329.
5. M. Reiss, *Ueber eine Steinersche combinatorische Aufgabe*, J. reine und angew. Math., *56* (1859), 326–344.
6. J. Steiner, *Combinatorische Aufgabe*, J. reine und angew. Math., *45* (1853), 181–182; also, *Gesammelte Werke* II (Berlin, 1884), pp. 435–436.
7. E. Witt, *Ueber Steinersche Systeme*, Abh. Math. Sem. Hamburg, *12* (1938), 265–275.
8. G. Tarry, *Le problème des 36 officiers*, C. R. Assoc. Franc. Av. Sci., *1* (1900), 122–123, *2* (1901), 170–203.

Technion, Israel Institute of Technology, Haifa

A METRIZATION FOR POWER-SETS WITH APPLICATIONS TO COMBINATORIAL ANALYSIS

ROBERT SILVERMAN

1. Introduction. Combinatorial configurations may generally be phrased in terms of arrangements of objects into sets subject to certain conditions. In view of this, the question arises as to whether given a set S and its power-set U_S (the class of all subsets of S), it might be possible to structure U_S in a combinatorially significant manner. This paper proposes and investigates one such structuring achieved by defining a distance function over U_S.

Given A, B in U_S, define their *distance* by

$$d(A, B) = N([A \cup B] - [A \cap B])/2,$$

where $N(E)$ denotes the number of elements in E, $+\infty$ being an admissible value. One readily verifies that the distance function satisfies the metric postulates $d(A, B) = 0$ if and only if $A = B$, and $d(A, B) \leqslant d(A, C) + d(B, C)$ for all A, B, C in U_S **(15)**. More generally, we may define a higher dimensional metric by associating with every r-tuple $E_1, \ldots, E_r$ of elements of U_S, the number $d(E_1, \ldots, E_r) = N(\cup A_i - \cap A_i)/r$. Although it appears that this will be necessary in order to obtain metric characterizations of, for example, the theorem of Desargues, only the ordinary metric is studied here.

Given the sets $S_1, \ldots, S_k$, denote by

$$\pi S_i = S_1 \times S_2 \times \ldots \times S_k = \{(s_1, \ldots, s_k); s_i \in S_i\},$$

their Cartesian product of ordered k-tuples. Since πS_i may be viewed as a subclass of an appropriate power-set by identifying the *element* $(s_1, \ldots, s_k)$ with the *set* $\{(1, s_1), \ldots, (k, s_k)\}$, the above definition also yields a metrization for Cartesian products which may be restated: For x, y in πS_i, $x = (x_1, \ldots, x_k)$, $y = (y_1, \ldots, y_k)$, $d(x, y)$ is the number of subscripts i for which $x_i \neq y_i$, $i = 1, \ldots, k$.

Section 3 gives metric characterizations of some of the classical configurations and their generalizations, such as balanced incomplete block designs (and, in particular, v, k, λ configurations and projective planes) and orthogonal Latin squares and cubes. Section 4 sets forth some theorems for metrized Cartesian product spaces.

2. Definitions and notation. In order to reduce to a minimum the introduction of new terminology, wherever feasible the author has adopted

Received January 12, 1959. This work was sponsored in part by the Office of Ordnance Research. The paper is based largely on the author's Ph.D. dissertation submitted to the Ohio State University in 1958.

that used by Blumenthal **(4; 5)**, whose excellent books also nourished several interesting trains of thought. In the following, M denotes an abstract metric space, and E a subspace of M. Wherever applicable, $+\infty$ is regarded as an admissible value.

DEFINITION 1. If $M = \{a_1, a_2, \ldots,\}$ is countable, it may be completely specified by the symmetric *distance matrix*

$$A = [a_{ij}], a_{ij} = d(a_i, a_j).$$

DEFINITION 2. For a in M, $r > 0$, the *open sphere* and *closed sphere with centre a, radius r* are defined, respectively, by

$$s(a, r) = \{x; x \text{ in } M, d(x, a) < r\},$$

$$c(a, r) = \{x; x \text{ in } M, d(x, a) \leqslant r\}.$$

Note that in general a sphere need not have a unique centre or radius.

DEFINITION 3. For x in M, the *distance of x from E* is given by $d(x, E) =$ g.l.b. $d(x, y)$ for y in E.

DEFINITION 4. Two metric spaces M and M' are *isometric* provided there exists a mapping α from M onto M' such that $d(x, y) = d(\alpha(x), \alpha(y))$ for all x, y in M. We write $M \sim M'$. Note that α is biunique since $\alpha(x) = \alpha(y)$ implies $d(\alpha(x), \alpha(y)) = d(x, y) = 0$. If $M = M'$, the isometry is termed a *motion*. Two subsets of M are *superposable* provided a motion exists that maps one onto the other.

DEFINITION 5. E is a *metric basis* of M provided each point of M is uniquely determined by its distances from the points of E.

DEFINITION 6. The *major diameter* $\Delta(E)$, of E, and the *minor diameter* $\delta(E)$, of E are defined by

$$\Delta(E) = \text{l.u.b. } d(x, y) \text{ for } x, y \text{ in } E,$$

$$\delta(E) = \text{g.l.b. } d(x, y) \text{ for } x, y \text{ in } E, x \neq y.$$

If E contains fewer than two points, define $\delta(E) = 0$.

Combinatorial configurations generally are highly symmetric in various aspects of their structure. Searching for a means of obtaining some sort of "symmetrizing" condition in U_S, it was discovered that one way of achieving this is to require that U_S contain a "large" number of elements mutually "far apart." These considerations motivate the next definition.

DEFINITION 7. The *t-extent* of E, $e(E, t)$, is the greatest integer m such that E contains m distinct points with minor diameter greater than t. If no two points of E have distance greater than t, set $e(E, t) = 1$, while if for n arbitrarily large there are n points of E with minor diameter exceeding t, define $e(E, t) = +\infty$.

As we shall see in the next section, the concept of t-extent enables us to give simple metric characterizations of the various configurations examined there.

Let $S(n)$ denote a set of n elements ($n > 1$), and $S^k(n)$ ($k \geqslant 1$) the k-fold Cartesian product of $S(n)$,

$$S^k(n) = \{(x_1, \ldots, x_k); x_i \in S(n)\}.$$

Assume that $S^k(n)$ has been metrized as in the preceding section, so that for x, y in $S^k(n)$, $x = (x_1, \ldots, x_k)$, $y = (y_1, \ldots, y_k)$, $d(x, y)$ is the number of subscripts i for which $x_i \neq y_i$, $i = 1, \ldots, k$. For $0 \leqslant r \leqslant k$, every set of $n^r + 1$ elements of $S^k(n)$ has minor diameter at most $k - r$. Hence the $k - r$ extent of every subspace E of $S^k(n)$ satisfies $e(E, k - r) \leqslant n^r$. We next define terms to describe subspaces which attain this maximum extent.

DEFINITION 8. A subspace E of $S^k(n)$ is *r-orthogonal*, $0 \leqslant r \leqslant k$, provided $e(E, k - r) = n^r$. If in addition E contains precisely n^r elements, E is termed an $L(n, k, r)$ space. (Thus E is r-orthogonal if and only if E contains an $L(n, k, r)$ space.)

For a given subspace E, r-orthogonality does not imply $(r - 1)$-orthogonality. $S^k(n)$ always has orthogonality 0, 1, and k. Indeed, any point constitutes an $L(n, k, 0)$ space; the points $(i, i, \ldots, i)$, $i = 1, \ldots, n$ comprise an $L(n, k, 1)$ space, and $S^k(n)$ is itself an $L(n, k, k)$ space. For values between 1 and k the property becomes non-trivial, and, as we shall see in the following section, is related to some of the classical unsolved problems in combinatorial analysis.

3. Metric characterizations of some combinatorial configurations.

(a) *Latin squares and cubes.* A *Latin square of order n*, $A = [a_{ij}]$, is an $n \times n$ matrix whose entries are from a set of n distinct symbols and such that each symbol appears exactly once in each row and column. Thus a Latin square of order n is essentially the multiplication table of a loop of order n. Two Latin squares $A = [a_{ij}]$, $B = [b_{ij}]$ of order n are *Graeco-Latin* provided the n^2 ordered pairs (a_{ij}, b_{ij}) are all distinct. A set of Latin squares of order n, $A_1, A_2, \ldots, A_m$, is *orthogonal* provided A_i and A_j are Graeco-Latin for all $i \neq j$. In this event, one readily shows that $m \leqslant n - 1$. An orthogonal set is *complete* provided $m = n - 1$.

A *Latin cube of order n*, $A = [a_{ijk}]$, i sa cubical array of n^3 cells (in n row-planes, n column-planes, and n layers) whose entries are from a set of n distinct symbols and such that whenever $a_{rst} = a_{uvw}$ and at least two of the equalities $r = u$, $s = v$, $t = w$ hold, then the third also holds. Note that this condition holds if and only if each row-plane, column-plane, and layer is a Latin square of order n. Two Latin cubes of order n are *Graeco-Latin* provided every pair of corresponding row-planes, column-planes, and layers is a Graeco-Latin square. Three Latin cubes, $A = [a_{ijk}]$, $B = [b_{ijk}]$, $C = [c_{ijk}]$,

of order n are *strongly Eulerian* provided each pair is Graeco-Latin and the n^2 ordered triples $(a_{ijk}, b_{ijk}, c_{ijk})$ are all distinct. (These conditions are stronger than those of Ball **(2)**.) A set of pairwise Graeco-Latin cubes of order n, $A_1, \ldots, A_m$, is *orthogonal* provided A_i, A_j, A_k are strongly Eulerian for all i, j, k pairwise distinct. Again one readily shows that $m \leqslant n - 1$, and an orthogonal set is termed *complete* provided $m = n - 1$.

There exists a fairly extensive literature on Latin squares. (In this connection, see the fine historical review by Norton **(19)**.) Euler conjectured that for $n = 4k + 2$, Graeco-Latin squares of order n do not exist, and Tarry **(25)** verified this for $n = 6$. Aside from $n = 6$ ($n = 2$ is, in a sense, vacuous since a complete set consists of a single square), the question of the validity of the conjecture has resisted all determined onslaught (although Mann **(17)** has ruled out certain candidates, among these being the group multiplication tables). The case $n = 10$ remains the first undecided instance.[1] MacNeish **(16)** seems to have been the first to establish the existence of complete sets of orthogonal Latin squares of prime power order. The interest in orthogonal Latin squares and finite projective planes was mutually enhanced when Bose **(6)** and Levi **(14)** independently showed the equivalence of complete sets of such squares to the planes.

Given a set of orthogonal Latin squares $A_1, \ldots, A_m$, of order n, construct the associated n^2 k-tuples ($k = m + 2$) in the usual manner. (Here the k-tuple $(i_1, \ldots, i_k)$ is admitted if and only if i_j is in row i_{k-1}, column i_k of A_j, $j = 1, \ldots, k - 2$.) One readily verifies that these n^2 elements actually comprise an $L(n, k, 2)$ space, since any pair of the elements having at least two corresponding components equal would violate either the Latin condition on rows or columns, or the orthogonality condition. Thus the minor diameter of the n^2 elements exceeds $k - 2$. Conversely, given an $L(n, k, 2)$ space, we may reverse the process and obtain $k - 2$ orthogonal Latin squares of side n. The same procedure may be employed to show the equivalence of $L(n, k, 3)$ spaces and sets of $k - 3$ orthogonal Latin cubes.

(b) *Finite nets.* For k, n positive integers with $k \geqslant 3$, Bruck **(9)** defines a (finite) net N of degree k, order n, as "a system of undefined objects called 'points' and 'lines' together with an incidence relationship ('point is on line' or 'line passes through point') such that:

(i) N contains k (non-empty) classes of lines.

(ii) Two lines a, b of N belonging to distinct classes, have a unique common point P.

(iii) Each point P of N is on exactly one line of each class.

(iv) Some line of N has exactly n distinct points.

"A finite affine plane with n points on each line, $n \geqslant 2$, is simply a net of degree $n + 1$, order n **(13)**. A loop of order n is essentially a net of degree 3, order n **(1; 3)**. More generally, for $3 \leqslant k \leqslant n + 1$, a set of $k - 2$ mutually

[1]See the addendum for recent developments.

orthogonal $n \times n$ Latin squares may be used to define a net of degree k, order n (and conversely) by paralleling Bose's correspondence **(6)** between affine planes and complete sets of orthogonal Latin squares."

For $k > r > 1$ we may generalize Bruck's configuration to a finite net of degree k, order n, and dimension r by replacing (ii) and (iv) with

(ii′) Every r lines $l_1, \ldots, l_r$ of N belonging to pairwise distinct classes have a unique common point P.

(iv′) Some line of N has exactly n^{r-1} points.

As immediate consequences of the axioms we have

(1) Every class contains n lines.

(2) Every line has exactly n^{r-1} points.

(3) N contains n^r points.

For let $A_1, \ldots, A_r, A_{r+1}, \ldots, A_k$ be the k classes of lines of N, and suppose A_i contains m_i lines, and N contains m points. One readily shows m_i and m to be finite. Then from (ii′) and (iii) we obtain the system of $r + 1$ equations $\pi m_j = m (j = 1, \ldots, r + 1, j \neq i; i = 1, \ldots, r + 1)$ which have the unique solution $m_i = m^{1/r}$, $i = 1, \ldots, r + 1$, and since we may replace A_{r+1} by any other A_j, we obtain $m_i = m^{1/r}$, $i = 1, \ldots, k$. If we next consider any fixed line of A_1 together with the classes $A_2, \ldots, A_r$, then (ii′) and (iii) imply that the line passes through $m^{(r-1)/r}$ points, and this together with (iv′) implies $m = n^r$.

Now let us co-ordinatize N by assigning to the point P the co-ordinates $(i_1, \ldots, i_k)$ provided P is on the i_jth line of the jth class. Then (ii′) and (iii) imply that there is a 1-1 correspondence between points and co-ordinates, and that as elements of $S^k(n)$ any two of these ordered k-tuples have distance exceeding $k - r$. Since there are n^r distinct such k-tuples, and each component of a k-tuple can assume n values, the n^r k-tuples comprise an $L(n, k, r)$ space. Conversely, one may reverse the above process, and we thus have a correspondence between $L(n, k, r)$ spaces with $1 < r < k$ and finite nets of degree k, order n, dimension r. In particular then, an $L(n, 3, 2)$ space is essentially a loop of order n, an $L(n, n + 1, 2)$ space defines a finite affine plane with n points on each line ($n \geqslant 2$), and from an $L(n, k, 2)$ space we may construct a system of $k - 2$ orthogonal Latin squares of side n.

(c) *Hypercubes and orthogonal arrays.* Rao **(21)** defines a hypercube of strength d as follows: "Let there be m factors $A_1, A_2, \ldots, A_m$ each of which can assume s different values. We define an ordered set $(i_1, i_2, \ldots, i_m)$ as a combination of m factors obtained by the selection of i_1th, i_2th ... values of the first, second, ..., factors respectively. There are s^m such combinations of which a subset of s^t combinations may be called a (m, s, t) array. An (m, s, t) array is said to be of strength d if all combinations of any d of the m factors occur in equal number (s^{t-d}) of times. An array of strength d represented by (m, s, t, d) is, alternatively, called a hypercube of strength d." For $t = d$, these hypercubes correspond to $L(n, k, r)$ spaces with $n = s$, $r = d$, and conversely.

Bose and Bush **(7, 8)** weakened the condition of s^t combinations to $N = \lambda s^d$ combinations, to obtain an orthogonal array of strength d, size N, index λ, k constraints, and s levels which they define as "a $k \times N$ matrix A, with entries from a set Σ of $s \geqslant 2$ elements . . . [such that] each $d \times N$ submatrix of A contains all possible $d \times 1$ column vectors with the same frequency λ." For $\lambda = 1$ it is clear that the column vectors of A comprise an $L(n, k, r)$ space, and conversely.

(d) *A configuration.* Let v elements be arranged into $v + 1$ sets $T_1, \ldots, T_{v+1}$ such that for $i \neq j$, the number of elements which are in either T_i or T_j but not in both is k. We may co-ordinatize the *sets* of the configuration by assigning to a set the co-ordinates $(i_1, \ldots, i_v)$, where $i_j = 1$ if the jth element is in the set, and $i_j = 0$ otherwise. If $x_1, \ldots, x_{v+1}$ are the co-ordinates of $T_1, \ldots, T_{v+1}$, respectively, then the x_i comprise a subspace of $S^v(2)$, $S(2) = \{0, 1\}$, satisfying $d(x_i, x_j) = k$, for all $i \neq j$. We will discuss this configuration further in the next example.

As an illustration, for $k = 4$, $v = 7$, consider

$$T_1 = \{1, 2\} \qquad T_4 = \{1, 3, 6, 7\} \qquad T_7 = \{2, 4, 6, 7\}$$
$$T_2 = \{3, 4\} \qquad T_5 = \{1, 4, 5, 7\} \qquad T_8 = \{1, 2, 3, 4, 5, 6\}.$$
$$T_3 = \{5, 6\} \qquad T_6 = \{2, 3, 5, 7\}$$

(e) *The v, k, λ configuration.* Consider next the now classic v, k, λ configuration defined in Chowla and Ryser **(11)** as an arrangement of v elements into v sets such that every set contains exactly k distinct elements and such that every pair of sets has exactly λ elements in common, $0 < \lambda < k < v$. In statistics these configurations are termed symmetrical balanced incomplete block designs. For $\lambda = 1$ and $k = n + 1$, $n \geqslant 2$, the configuration reduces to a projective plane with $n + 1$ points per line, and for $v = 4m - 1$, $k = 2m - 1$, $\lambda = m - 1$, it is equivalent to a Hadamard matrix of order $N = 4m$ **(20)** (these are the ± 1 matrices H satisfying $HH^T = NI$, where H is of order N and I is the identity matrix). For a comprehensive summary of results see Ryser **(22)**. With the v, k, λ configuration we may associate its characterizing $v \times v$ incidence matrix $A = [a_{ij}]$, where $a_{ij} = 1$ if the jth element is in the ith set, and 0 otherwise. Actually, constructing the incidence matrix is equivalent to co-ordinatizing the sets of the configuration, the ith row representing the co-ordinates of the ith set. It is apparent that the v sets of co-ordinates so obtained comprise v elements of $S^v(2)$, $S(2) = \{0, 1\}$, satisfying:

(i) If $s = (0, 0, \ldots, 0)$, and the v elements are $x_1, \ldots, x_v$, then $d(x_i, s) = k$ for $i = 1, \ldots, v$.

(ii) $d(x_i, x_j) = 2(k - \lambda)$, $i \neq j$.

That the metric characterization of v, k, λ tends toward the heart of the matter is suggested in (ii) by the fact that the value $k - \lambda$ which appears in both the v, k, λ design and its complementary design (the design obtained

by replacing each set by its complement) and plays such a critical role in the non-existence theorems, occurs explicitly.

Also of interest is the fact that the "strong" converse of the above holds. That is, given $v + 1$ elements $s', x_1', \ldots, x_v'$ of $S^v(2)$ satisfying

(i') $d(x_i', s') = k$ for $i = 1, \ldots, v$

(ii) $d(x_i', x_j') = 2(k - \lambda)$, $i \neq j$, $0 < \lambda < k < v$,

we may construct v elements $x_1, \ldots, x_v$ satisfying (i) and (ii) and hence constituting a v, k, λ configuration. This may be seen as follows. If in the jth components of $x_1', \ldots, x_v', s'$ we replace 0's by 1's and 1's by 0's, we clearly obtain an isometric space. Now perform this replacement in the jth components if and only if the jth component of s' is 1. Then we obtain an isometric space with $s = (0, 0, \ldots, 0)$ as the image of s'.

Consider again the configuration in (d). Though, at least on the surface, the relation of this configuration to the v, k, λ configuration is somewhat obscure, by relating both to their metric characterizations, it is immediately apparent that for $0 < 2\lambda = k < v$, they are essentially equivalent.

(f) *Balanced incomplete block designs.* Let $T = \{s_1, \ldots, s_v\}$, and consider the configuration $C = \{T_1, \ldots, T_b\}$, where the T_i are subsets of T. Then the *dual* configuration consists of the subsets $A_1, \ldots, A_v$ of the set $A = \{t_1, \ldots, t_b\}$, where t_i is in A_j if and only if a_j is in T_i; and the *complementary* configuration consists of the sets $\bar{T}_1, \ldots, \bar{T}_b$, where $\bar{T}_i$ denotes the complement of T_i.

Given the set $S(b)$ of b elements, let E_r denote the class of all subsets of $S(b)$ containing r elements. Then E_r is a subspace of the metric space $U_{S(b)}$. We will show that for $0 < \lambda < r < b$, the existence of a balanced incomplete block design BIBD **(26)** with parameters b, v, k, r, λ is equivalent to having $e(E_r, r - \lambda - 1) = (r - \lambda)b/(r^2 - \lambda b)$ with $r^2 - \lambda b > 0$.

THEOREM 3.1. *If* $r^2 - \lambda b > 0$ (λ *integral and* $0 \leqslant \lambda < r$), *then*

(a) $e(E_r, r - \lambda - 1) \leqslant v$, *where* $v = (r - \lambda)b/(r^2 - \lambda b)$.

(b) *Equality holds in* (a) *if and only if there exist* v *elements* $x_1, \ldots, x_v$ *in* E_r *such that* $d(x_i, x_j) = r - \lambda$, *for all* $i \neq j$.

Proof. Let $e(E_r, r - \lambda - 1) = m$. Then since λ is integral there exist $x_1, \ldots, x_m$ in E_r with $d(x_i, x_j) \geqslant r - \lambda$ for all $i \neq j$. Denote by k_i the number of sets x_j containing the ith element of $S(b)$, $i = 1, \ldots, b$. Comparing total occurrences we obtain

$$\sum k_i = rm. \tag{1}$$

Comparing contributions to all

$$\binom{m}{2}$$

set intersections, we obtain

$$\sum \binom{k_i}{2} = \sum_{i<j} N(x_i \cap x_j) = \sum_{i<j} [r - d(x_i, x_j)]. \tag{2}$$

But then $d(x_i, x_j) \geqslant r - \lambda$ implies

$$\sum \binom{k_i}{2} \leqslant \lambda \binom{m}{2}. \tag{3}$$

Now from Lemma 1 (§ 4) and (1), (3) follows

$$L = b\binom{rm/b}{2} \leqslant M = \sum \binom{k_i}{2} \leqslant R = \lambda \binom{m}{2}. \tag{4}$$

Using $r^2 - \lambda b > 0$, we find from elementary calculations that $L \leqslant R$ is equivalent to $m \leqslant v$, and $L = R$ if and only if $m = v$. Thus conclusion (a) is established. Finally, if $m = v$, from $L = M = R$ and (2) it follows that

$$\sum [r - d(x_i, x_j)] = \lambda \binom{m}{2},$$

and thus $d(x_i, x_j) \geqslant r - \lambda$ implies $r - d(x_i, x_j) = \lambda$. Hence $d(x_i, x_j) = r - \lambda$, completing the proof of the theorem.

COROLLARY 1. For $0 < \lambda < r < b$, the configuration $x_1, \ldots, x_v$ is the dual of a BIBD with parameters b, v, k, r, λ, where $k = rv/b$. Conversely, given the BIBD and considering its dual configuration as a subspace of E_r, one obtains $e(E_r, r - \lambda - 1) = v$, $r^2 - \lambda b > 0$, and $v = (r - \lambda)b/(r^2 - \lambda b)$.

Proof. In the proof of the above theorem, from $m = v$ we obtain $L = M$. This together with Lemma 1 (§ 4) and (1), gives $k_i = rv/b = k$, for $i = 1, \ldots, b$. Thus every element of $S(b)$ occurs in k of the sets $x_1, \ldots, x_v$. Further, note that $d(x_i, x_j) = r - \lambda$ for all $i \neq j$ implies that every pair of distinct sets intersect in exactly λ elements. Thus the first conclusion follows. Conversely, given the BIBD and considering its dual configuration as a subspace of E_r, one obtains $e(E_r, r - \lambda - 1) \geqslant v$. Further, from $0 < \lambda < r < b$, and the well-known conditions $rv = bk$, $\lambda(v - 1) = r(k - 1)$, it follows that $r^2 - \lambda b > 0$ and $v = (r - \lambda)b/(r^2 - \lambda b)$. But then from conclusion (a) of the theorem, we have $e(E_r, r - \lambda - 1) = v$.

Specializing to v, k, λ configurations, one obtains the interesting result:

COROLLARY 2. *If v elements are arranged in $v' \geqslant v$ sets of k elements each, such that every pair of distinct sets has at most λ elements in common, where $\lambda < k^2/v$ is a non-negative integer, then $\lambda \geqslant k(k - 1)/(v - 1)$. If equality holds, then $v' = v$ and every pair of distinct sets has exactly λ elements in common.*

Thus for $1 < k < v$, the arrangement constitutes a v, k, λ configuration. (In this event, it is interesting to note that from Corollary 1 one also obtains directly that each element occurs in exactly k sets.)

Proof. From conclusion (a) of the theorem we have that if $k^2 - \lambda v > 0$, then $v \leqslant v' \leqslant e(E_k, k - \lambda - 1) \leqslant (k - \lambda)v/(k^2 - \lambda v)$. But $v \leqslant (k - \lambda)v/(k^2 - \lambda v)$ is equivalent to $\lambda \geqslant k(k - 1)/(v - 1)$, and equality hold sin both expressions or neither. Finally, apply the proof of (b).

4. Some theorems for metrized Cartesian product spaces. Let E_i denote a subspace of the metric space $S^k(n_i)$, $i = 1, \ldots, t$. For $x_i = (a_{i1}, \ldots, a_{ik})$ in E_i, $i = 1, \ldots, t$, let $x_1x_2 \ldots x_t = \pi x_i = (b_1, \ldots, b_k)$, where $b_j = (a_{1j}, \ldots, a_{tj})$, $j = 1, \ldots, k$. If $\pi x_i = (b_1, \ldots, b_k)$, $\pi y_i = (c_1, \ldots, c_k)$, x_i and y_i in E_i, define $d(\pi x_i, \pi y_i)$ in the usual manner as the number of subscripts j for which $b_j \neq c_j$, $j = 1, \ldots, k$.

Definition 9. The metric space

$$E_1\dot{x}E_2\dot{x} \ldots \dot{x}E_t = \dot{\pi}E_i = \{\pi x_i; x_i \in E_i\}$$

is termed the *direct product* of the E_i. Note the distinction between the *direct* product $\dot{\pi}E_i$ and the *Cartesian* product πE_i.

From the above definition, it is clear that any biunique mapping from $\pi S(n_i)$ onto $S(\pi n_i)$ induces an isometry between $\dot{\pi}S^k(n_i)$ and $S^k(\pi n_i)$. For convenience we simply write $\dot{\pi}S^k(n_i) = S^k(\pi n_i)$. With this understanding, $\dot{\pi}E_i$ is a subspace of $S^k(\pi n_i)$. Note that the direct product is independent of the order of the factors. That is, if $i(1), \ldots, i(t)$ is a permutation of $1, 2, \ldots, t$, then $\dot{\pi}E_j$ is isometric to $\dot{\pi}E_{i(j)}$ under the mapping $\pi x_j \to \pi x_{i(j)}$. Next note that if $t_1 < t_2 < \ldots < t_r = t$, then $\dot{\pi}E_{i(1)}\dot{x}\dot{\pi}E_{i(2)}\dot{x} \ldots \dot{x}\dot{\pi}E_{i(r)}$ is isometric to $\dot{\pi}E_j$, where $i(j) = t_{j-1} + 1, \ldots, t_j$ $(t_0 = 0)$. In particular it follows that $(E_1\dot{x}E_2)\dot{x}E_3$ and $E_1\dot{x}(E_2\dot{x}E_3)$ are isometric since each is isometric to $E_1\dot{x}E_2\dot{x}E_3$. Thus, relative to isometry, the direct product operation is associative and commutative.

THEOREM 4.1. *For x_i and y_i in E_i,*

$$\max[d(x_i, y_i)] \leqslant d(\pi x_i, \pi y_i) \leqslant \sum d(x_i, y_i).$$

Proof. From the definition it is clear that if x_r and y_r have distinct jth components, then so do πx_i and πy_i. Hence $d(x_r, y_r) \leqslant d(\pi x_i, \pi y_i)$ and the first inequality follows. Next suppose πx_i and πy_i have distinct jth components. Then so do at least one pair x_i, y_i, and from this it is clear that the second inequality must hold.

COROLLARY 1. *The major and minor diameters Δ, δ satisfy*

$$\max(\delta(E_i)) \leqslant \delta(\dot{\pi}E_i) \leqslant \Delta(\dot{\pi}E_i) \leqslant \Sigma\Delta(E_i).$$

Proof. From the definitions and the theorem we have

$$\delta(E_i) \leqslant d(x_i, y_i) \leqslant \max d(x_i, y_i) \leqslant d(\pi x_i, \pi y_i),$$

which implies $\max \delta(E_i) \leqslant \delta(\dot{\pi}E_i)$. Also

$$d(\pi x_i, \pi y_i) \leqslant \sum d(x_i, y_i) \leqslant \sum \Delta(E_i)$$

implies that $\Delta(\dot{\pi}E_i) \leqslant \sum \Delta(E_i)$.

COROLLARY 2. *If $S^k(n_1)$ and $S^k(n_2)$ are r-orthogonal, then so is $S^k(n_1n_2)$.*

Proof. Let L_i be an $L(n_i, k, r)$ space of $S^k(n_i)$, $i = 1, 2$. Then $L = L_1 \dot{x} L_2$ is an $L(n_1 n_2, k, r)$ space of $S^k(n_1 n_2)$, since

$$\delta(L) \geqslant \max[\delta(L_1), \delta(L_2)] > k - r,$$

and L contains exactly $(n_1 n_2)^r$ elements.

By identifying the element $(a_1, \ldots, a_k)$ with the set $\{(1, a_1), \ldots, (k, a_k)\}$, we can apply Theorem 3.1 and its first corollary to the metric space $S^k(n)$. We then obtain immediately

THEOREM 4.2. *If $k > (r-1)n$ (r integral, $2 \leqslant r$, $n > 1$), then*

(a) $e(S^k(n), k - r) \leqslant v$, where $v = n[k - (r-1)]/[k - n(r-1)]$.

(b) *If equality holds in* (a) *there exist v elements $x_1, \ldots, x_v$ in $S^k(n)$ such that $d(x_i, x_j) = k - (r-1)$, for all $i \neq j$. In this event, each element of $S(n)$ occurs as a jth component of exactly $t = [k - (r-1)]/[k - n(r-1)]$ of the x_i's, $j = 1, \ldots, k$. Further, from $x_1, \ldots, x_v$ we can construct a* BIBD *with parameters b', v', k', r', λ' $(0 < \lambda' < r' < b')$, where $b' = kn$, $v' = v$, $k' = t$, $r' = k$, $\lambda' = r - 1$.*

This BIBD has the special property that its b' blocks can be partitioned into k pairwise disjoint classes of n blocks each, such that every variety occurs in exactly one block from each class. Conversely, given such a BIBD, one can construct v elements of $S^k(n)$ with mutual distances exceeding $k - r$, and the elementary conditions on its parameters will imply $k > (r-1)n$.

From Cauchy's inequality we obtain

LEMMA 1. *For the real numbers $a_1, \ldots, a_n$,*

$$n\binom{a}{2} \leqslant \sum \binom{a_i}{2},$$

where

$$\binom{a_i}{2} = a_i(a_i - 1)/2$$

and $a = (\sum a_i)/n$. Further, equality holds if and only if $a_i = a$ for all i.

LEMMA 2. *Let $i(1), \ldots, i(t)$, $t \leqslant r$, be any t distinct integers from among $1, \ldots, k$, and let $a_{i(j)}$ be in $S(n)$. Then in the $L(n, k, r)$ space, L, there are precisely n^{r-t} elements with $i(j)$th component equal to $a_{i(j)}$, $j = 1, \ldots, t$.*

Proof. The proof is evident from the fact that L contains n^r elements, any two distinct elements agree in at most $r - 1$ corresponding components, and over $S(n)$ every t-tuple can be completed to an r-tuple in exactly n^{r-t} ways.

LEMMA 3. *If $S^k(n)$ is r-orthogonal, then $S^{k-1}(n)$ is $(r-1)$-orthogonal.*

Proof. Let L be an $L(n, k, r)$ space of $S^k(n)$. By Lemma 2 there are n^{r-1} elements in L having the same kth component. If their kth components are dropped, it is easy to see that the n^{r-1} elements so obtained constitute an $L(n, k-1, r-1)$ space.

LEMMA 4. *If $S^k(n)$ is r-orthogonal, then so is $S^t(n)$, $t < k$.*

Proof. This is clear from the fact that if the last $k-t$ components of the elements in an $L(n, k, r)$ space are dropped, the resulting elements comprise an $L(n, t, r)$ space.

LEMMA 5. *If $S^k(n)$ is r-orthogonal, $r \geqslant 2$, then $k \leqslant n + r - 1$.*

Proof. Let L be an $L(n, k, r)$ space in $S^k(n)$. For a in $S(n)$, by Lemma 2 there are n elements $x_1, \ldots, x_n$ in L with first $r-1$ components equal to a, and an element x_{n+1} distinct from these and having its first $r-2$ components equal to a. Thus from $d(x_i, x_j) > k - r$ for all $i \neq j$, it follows that $n \geqslant k - r + 1$.

LEMMA 6. *For x and y in the $L(n, n + r - 1, r)$ space, L, $d(x, y) \leqslant n + 1$ implies $d(x, y) = n$.*

Proof. Let $x = (a_1, \ldots, a_k)$, $y = (b_1, \ldots, b_k)$, $k = n + r - 1$. Suppose $d(x, y) \leqslant n + 1$. Then $a_i = b_i$ for at least $r - 2$ subscripts i. With no loss of generality, suppose $a_i = b_i$, $i = 1, \ldots, r-2$. Now by Lemma 2 there are exactly $n^2 - 1$ elements in $L(n, k, r)$ which are different from x and have ith component equal to a_i, $i = 1, \ldots, r-2$. Let A_j denote the subset of these $n^2 - 1$ elements having jth component equal to a_j, $j = r-1, \ldots, k$. Then again by Lemma 2, A_j contains precisely $n - 1$ elements. Also, $A_i \cap A_j = \phi$ for $i \neq j$, and so $\cup A_j$ contains precisely $(n-1)(n+1) = n^2 - 1$ elements. Thus every element in L having ith component equal to a_i, $i = 1, \ldots, r-2$, has its jth component equal to a_j for precisely one value of j, $r - 1 \leqslant j \leqslant k$, and so has distance n from x. In particular, $d(x, y) = n$.

LEMMA 7. *Given a $k \times r$ matrix, A, over a field F, having all its r-rowed minors non-singular, we can construct a $k \times (k-r)$ matrix with all $(k-r)$-rowed minors non-singular.*

Proof. Let A_1 denote the $r \times r$ matrix consisting of the first r rows of A, and let A_2 denote the $(k-r) \times r$ matrix consisting of the remaining $k - r$ rows, so that

$$A = \begin{bmatrix} A_1 \\ A_2 \end{bmatrix}.$$

By hypothesis A_1 is non-singular, so by elementary operations on the columns of A we can obtain

$$A' = \begin{bmatrix} I \\ A_2' \end{bmatrix},$$

where I is the $r \times r$ identity matrix. Since the elementary operations have been performed only on the *columns* of A, A' also has all r-rowed minors non-singular. Now using the Laplace expansion, one sees that every minor determinant of A_2' occurs as a factor of some r-rowed minor determinant of A', and hence is not zero. Again applying the Laplace expansion, one verifies that every $(k-r)$-rowed minor determinant of the $(k-r) \times k$ matrix $[A_2', I]$ either equals unity or has the same absolute value as some minor determinant of A_2' (here I is the $(k-r)$-rowed identity matrix). Hence $[A_2', I]$ has all $(k-r)$-rowed minors non-singular. Taking the transpose, we have the required result.

THEOREM 4.3. *Given a $k \times r$ matrix $A = [a_{ij}]$ over $GF(p^m)$ having all r-rowed minors non-singular, we can construct an $L(n, k, r)$ and an $L(n, k, k-r)$ space, $n = p^m$.*

Proof. Denote the row vectors of A by $\alpha_1, \ldots, \alpha_k$. Let $L = \{Ax\}$, where x ranges over the n^r r-place column vectors over $GF(p^m)$. Then L is an $L(n, k, r)$ space, for suppose $Ax, Ay, x \neq y$, have as many as r components the same, say $i(1), \ldots, i(r)$. Then the submatrix B of A consisting of the row vectors $\alpha_{i(1)}, \ldots, \alpha_{i(r)}$ satisfies $Bx = By$. But by hypothesis B is non-singular, so $x = y$ contradicting our choice of x and y. Hence $d(Ax, Ay) > k - r$, and L is an $L(n, k, r)$ space. Finally, by Lemma 7, from A we can construct a $k \times (k-r)$ matrix with all r-rowed minors non-singular, and applying the above proof we obtain an $L(n, k, k-r)$ space.

The first part of the above theorem corresponds to that of Bose and Bush (**7**, Theorem 5A, p. 521) with index one. They employ a similar proof.

LEMMA 8. *For $n = p^m$, p a prime,*

(1) *$S^k(n)$ is r-orthogonal for $k \leqslant n + 1$.*
(2) *$S^k(n)$ is 3-orthogonal for $k \leqslant n + 2$ and $p = 2$.*
(3) *$S^k(n)$ is r-orthogonal for $k \leqslant r + 1$.*

Proof. Letting $a_1, \ldots, a_{n-1}$ denote the non-zero elements of $GF(p^m)$, one readily verifies that the matrix

$$\begin{bmatrix} B \\ 1\,0 \ldots 0\,0 \\ 0\,0 \ldots 0\,1 \end{bmatrix}$$

where $B = [b_{ij}]$ is an $(n-1) \times r$ matrix with $b_{ij} = a_i^j$, $j = 0, \ldots, r-1$, has all r-rowed minors non-singular, since their determinants all reduce to the Vandermonde type. For the special case $p = 2$, $r = 3$, we may adjoin to A as an $(n+2)$th row the vector $(0, 1, 0)$ and again verify that A has all 3-rowed minors non-singular. Conclusions (1) and (2) now follow from Theorem 4.3 and Lemma 4. Finally, consider (3). For $k = r$, the result is trivial. For $k = r + 1$, the matrix obtained by adjoining the row vector

$(1, 1, \ldots, 1)$ to the $r \times r$ identity matrix has all r-rowed minors non-singular, and (3) follows from Theorem 4.3.

Conclusions (1) and (2) of the above lemma correspond to the theorem of Bush **(8**, p. 431**)**, who obtains the construction by employing polynomials over $GF(p^m)$.

From Lemmas 4 and 8 and Corollary 2 of Theorem 4.1, we obtain

THEOREM 4.4. *If $n = \pi p_i^{e_i}$ is the decomposition of n into distinct prime powers, then*

(1) *$S^k(n)$ is r-orthogonal for $k \leqslant \min(p_i^{e_i} + 1)$.*
(2) *$S^k(n)$ is 3-orthogonal for $k < 2^m + 2$ if $\min(p_i^{e_i} + 1) = 2^m + 1$.*
(3) *$S^k(n)$ is r-orthogonal for arbitrary n whenever $k \leqslant r + 1$.*

From the relation between orthogonal Latin squares and $L(n, k, 2)$ spaces, for $r = 2$ we obtain the theorem proved in Mann's book **(18**, Theorem 8.8, p. 105**)** (other construction methods may be found in **(16**, Theorem 12.1**)**):

COROLLARY. *There exist at least $\min(p_i^{e_i} - 1)$ orthogonal Latin squares of side $n = \pi p_i^{e_i}$.*

(It is of interest to note here that in a yet unpublished paper, E. T. Parker has, by an elegant construction, succeeded in exceeding the minimum given in the above corollary for certain values of n. The author believes this to be the first such successful attempt.)

THEOREM 4.5. *Let L be an $L(n, k, r)$ space, $r \geqslant n - 1$, $k \geqslant r + 2$. Then $r = n - 1$, and for every x in $S^k(n)$, $d(x, L) < k - r$.*

Proof. Let $x = (x_1, \ldots, x_k)$, and applying Lemma 2 with $t = r$, let $y = (a_1, \ldots, a_k)$ be the unique element of L having $a_i = x_i$, $i = 1, \ldots, r$. Let $y' = (a_1, \ldots, a_r)$, and in $S^r(n)$ consider the unit closed sphere $c(y', 1)$. The sphere contains $r(n - 1)$ elements $y_1', \ldots, y_{r(n-1)}'$ different from y', and by the triangle inequality, $d(y_i', y_j') \leqslant 2$, $i \neq j$. Again by Lemma 2, to each $y_i' = (b_{i1}, \ldots, b_{ir})$ there corresponds a unique element y_i in L, $y_i = (b_{i1}, \ldots, b_{ir}, u_i, v_i, \ldots,)$. Now $d(y, y_i) > k - r$ and $d(y', y_i') = 1$ imply $u_i \neq a_{r+1}$, $v_i \neq a_{r+2}$. Also, for $i \neq j$, $d(y_i, y_j) > k - r$ and $d(y_i', y_j') \leqslant 2$ imply that the ordered pairs (u_i, v_i) and (u_j, v_j) are distinct. Thus there are $r(n - 1)$ distinct ordered pairs (u_i, v_i) for which $u_i \neq a_{r+1}$ and $v_i \neq a_{r+2}$. But since the total number of such pairs is $(n - 1)^2$, we must have $r(n - 1) \leqslant (n - 1)^2$ or $r \leqslant n - 1$. Hence $r = n - 1$.

We now prove the second part of the theorem. If $x_i = a_i$ for either $i = r + 1$ or $r + 2$, we are done. So assume $x_i \neq a_i$, $i = r + 1$, $r + 2$. But then (x_{r+1}, x_{r+2}) must be one of the pairs (u_i, v_i), and the conclusion follows.

As an immediate corollary, we obtain the equivalent of the theorem of Bush **(8**, p. 427**)**:

COROLLARY 1. *If $S^k(n)$ is r-orthogonal, then $r \geqslant n$ implies $k \leqslant r + 1$.*

(Thus there are no Graeco-Latin squares of order 2, no Graeco-Latin cubes of order 3, etc.)

Lemma 5 and the above corollary give

COROLLARY 2. *For* $1 < r < k - 1$ *and* $k \geqslant 2n - 1$, $S^k(n)$ *is not* r*-orthogonal.*

THEOREM 4.6. *If* $S^k(n)$ *is* r*-orthogonal for* $r \geqslant 2$ *and* $k = n + r - 1$, *then*

$$\binom{n + t - 3}{t - 2} \equiv 0 \bmod (t - 1) \text{ for } t = 2, 3, \ldots, r.$$

Proof. The proof is by induction on r. For $r = 2$ the theorem is trivial. Assume the theorem holds for $r - 1$, $r \geqslant 3$. Let L be an $L(n, k, r)$ space, and let $x = (a_1, \ldots, a_k)$ be in L, $k = n + r - 1$. By Lemma 2, L contains n^{r-2} elements y_j, $j = 1, \ldots, n^{r-2}$, with first and second components b_1 and b_2, respectively, $b_1 \neq a_1$, $b_2 \neq a_2$. Also, for every set $i_1, \ldots, i_{r-2}$ of $r - 2$ distinct integers from among $3, 4, \ldots, n + r - 1$, there is a unique element $y(i_1, \ldots, i_{r-2})$ among the y_j's with i_jth component equal to $a_{i(j)}$ $(i(j) = i_j)$, $j = 1, \ldots, r - 2$. But then by Lemma 6, the distance of this element from x is n, and so among the last $n + r - 3$ components, $y(i_1, \ldots, i_{r-2})$ has $r - 1$ components equal to the corresponding components of x. Hence there are

$$\binom{r - 1}{r - 2} = r - 1$$

distinct sets $\{j_1, \ldots, j_{r-2}\}$ associated with the same element $y(i_1, \ldots, i_{r-2})$. Further, since x and $y(i_1, \ldots, i_{r-2})$ agree in at most $r - 1$ corresponding components, there can be no more than $r - 1$ such sets associated with $y(i_1, \ldots, i_{r-2})$. Thus the

$$\binom{n + r - 3}{r - 2}$$

sets are divided into classes of $r - 1$ sets each, and we must have

$$\binom{n + r - 3}{r - 2} \equiv 0 \bmod (r - 1).$$

Applying the induction hypothesis and Lemma 3, we obtain the theorem.

From $t = 3$ in the above, one obtains the theorem of Bush (**8**, p. 430):

COROLLARY. *For* n *odd,* $r \geqslant 3$, *an* $L(n, k, r)$ *space satisfies* $k \leqslant n + r - 2$.

Relative to our previous remarks (§ 3, Example (a)), from the above theorem and Lemma 8 it follows that complete sets of orthogonal Latin cubes always exist for n a power of 2, and never exist for n odd. However, for n an odd prime power $\geqslant 5$, we can always construct a complete set less one.

THEOREM 4.7. *If* $S^n(n)$ *is 2-orthogonal, then so is* $S^{n+1}(n)$.

Proof. Let L be an $L(n, n, 2)$ space in $S^n(n)$, where $S(n) = \{a_1, \ldots, a_n\}$. Denote by $x_1, \ldots, x_n$ the n elements of L having first component equal to a_1 (Lemma 2). Let x_i' in $S^{n+1}(n)$ be the element obtained by adjoining a_i as an $(n+1)$th component to x_i, $i = 1, \ldots, n$. Let y in L be different from the x_i's. Then since $d(x_i, x_j) = n - 1$ for all $i \neq j$, each a_j occurs exactly once as a tth component of the x_i's for $t = 2, \ldots, n$. Hence $d(x_i, y) > n - 2$ for $i = 1, \ldots, n$ implies that there is a unique subscript m for which $d(x_m, y) = n$. Let y' in $S^{n+1}(n)$ be the element obtained by adjoining a_m as an $(n+1)$th component to y. Now repeat the above process for all y in L different from the x_i's, and denote by L' the set of n^2 elements of $S^{n+1}(n)$ which are thus obtained. By construction it is clear that x_i' has distance n from each of the other elements of L'. Let y_1' and y_2' be any two distinct elements of L' different from the x_i''s. If $d(y_1, y_2) = n$, then $d(y_1', y_2') \geqslant n$. If y_1 and y_2 have the same first component $b \neq a_1$, let $y_3, \ldots, y_n$ denote the remaining elements of L with first component b. Then applying the argument used above to the y_i, for each x_i there is a unique subscript m for which $d(y_m, x_i) = n$. Hence, by construction, no two of the y_i''s have the same $(n+1)$th component, and so in particular, $d(y_1', y_2') = n$. Finally, if y_1 and y_2 have the same jth component b, $2 \leqslant j \leqslant n$, let $y_3, \ldots, y_{n-1}, x_i$ denote the remaining elements of L with jth component b. Again applying the above argument, we obtain $d(y_1', y_2') = n$. Hence $d(x', y') \geqslant n$ for all x', y' in L', and so L' is an $L(n, n+1, 2)$ space and $S^{n+1}(n)$ is 2-orthogonal.

The above theorem is equivalent to saying that every set of $n - 2$ orthogonal Latin squares of side n may be completed to a full set of $n - 1$ orthogonal Latin squares. From our remarks following Theorem 4.7, it is interesting to note that the corresponding theorem for cubes is false.

From Lemma 3, Theorem 4.7, the Bruck-Ryser non-existence theorem **(10)** and the relations among orthogonal Latin squares, projective planes, and $L(n, k, r)$ spaces, we obtain immediately:

THEOREM 4.8. *If $n \equiv 1$ or $2 \pmod 4$ and the square-free part of n is divisible by a prime of the form $4k + 3$, then $S^k(n)$ is not r-orthogonal for $k \geqslant n + r - 2$, $r \geqslant 2$.*

THEOREM 4.9. *If $S^k(n)$ is r-orthogonal, then it admits of a partitioning into pairwise disjoint, superposable $L(n, k, r)$ spaces.*

Proof. Suppose $S^k(n)$ is r-orthogonal, and let L denote an $L(n, k, r)$ space of $S^k(n)$. Let $A_1, \ldots, A_{k-r}$ be $k - r$ Latin squares of side n, and denote by $\alpha(i, j)$ the permutation $t \to a_t$, $t = 1, \ldots, n$, where $(a_1, a_2, \ldots, a_n)$ is the ith row vector of A_j. Finally, let $\omega = \omega(i_1, \ldots, i_{k-r})$ denote the mapping of $S^k(n)$ into itself generated by performing the permutation $\alpha(i_j, j)$ upon the jth components of the elements of $S^k(n)$, $j = 1, \ldots, k - r$. It is clear that ω is indeed a motion (Definition 4), and so under ω, L is carried into a superposable $L(n, k, r)$ space, $L(i_1, \ldots, i_{k-r})$. Further, from Lemma 2 with $t = r$,

it is easy to see that if $(i_1, \ldots, i_{k-r})$ and $(j_1, \ldots, j_{k-r})$ are distinct as vectors, then $L(i_1, \ldots, i_{k-r})$ and $L(j_1, \ldots, j_{k-r})$ are disjoint. Finally, since $L(i_1, \ldots, i_{k-r})$ consists of n^r elements, and there are n^{k-r} distinct vectors $(i_1, \ldots, i_{k-r})$, it is clear that these spaces exhaust $S^k(n)$.

THEOREM 4.10. *For $r > 1$, $L(n, k, r)$ is a metric basis for $S^k(n)$.*

Proof. The theorem is trivial for $k = r$, so assume $k > r$. Let x and y be arbitrary in $S^k(n)$, $x = (a_1, \ldots, a_k)$, $y = (b_1, \ldots, b_k)$, $x \neq y$. The theorem will be proved if it can be shown that (C): there exists z in $L(n, k, r)$ such that $d(x, z) < d(y, z)$. Proof is by induction on r. Consider first $L(n, k, 2)$. Suppose, say, $a_1 \neq b_1$. Let $z_1, \ldots, z_n$ be the n elements of $L(n, k, 2)$ with first component equal to a_1. If for some z_i, $d(y, z_i) = k$, we are done since $d(x, z_i) \leqslant k - 1$. So suppose $d(y, z_i) < k$ for $i = 1, \ldots, n$. Then since $L(n, k, 2)$ has minor diameter $\geqslant k - 1$, by Lemma 5 we must have $k = n + 1$, and hence $d(y, z_i) = k - 1$, $i = 1, \ldots, n$. Now let z_i be the unique element among the z_i (Lemma 2) with second component equal to a_2. Then $d(y, z_i) = k - 1$ and $d(x, z_i) \leqslant k - 2$. This completes the proof for $r = 2$. Now suppose that (C) holds for $r - 1 (r \geqslant 3)$ and all k, and consider $L(n, k, r)$. If $d(x, y) \leqslant r$, then by Lemma 2, we can always find a z in $L(n, k, r)$ such that $d(x, z) < d(y, z)$. So suppose $d(x, y) > r \geqslant 3$. Select the n^{r-1} elements in $L(n, k, r)$ with kth component equal to a_k. Denote these elements by $z_1, \ldots, z_t$, $t = n^{r-1}$, and let $z_1', \ldots, z_t'$ be the corresponding elements of $S^{k-1}(n)$ obtained by dropping the kth components of the z_i. By the proof of Lemma 3, the z_j''s constitute an $L(n, k - 1, r - 1)$ space, and by the induction hypothesis there exists z_i' in $L(n, k - 1, r - 1)$ with $d(x', z_i') < d(y', z_i')$, where $x' = (a_1, \ldots, a_{k-1})$, $y' = (b_1, \ldots, b_{k-1})$. But $d(x', z_i') = d(x, z_i)$, and $d(y', z_i') \leqslant d(y, z_i)$. Hence $d(x, z_i) < d(y, z_i)$.

5. Concluding remarks. The investigation of the metric properties of $S^k(n)$ and, in general, of power-sets has, of course, only its beginnings in the present paper. One of the initial problems is the discovery of further significant concepts (such as "extent" appears to be, for example), since many of the classical metric concepts apparently will have limited value, and topological concepts become completely trivial for the finite spaces. High on the list of desiderata would be a development of the basic theory to the point where the elements, say, of $S^k(n)$ could be treated abstractly, making it unnecessary to deal with their internal structure each time a new result is under scrutiny. For it is precisely at the point where internal combinatorial structure becomes too complex for the mind to grasp as a totality that our efforts fail.

A line of attack which has been neglected in the present paper and which may prove to be fruitful, is an examination of the distance matrix. One may readily obtain an indication of the manner in which some of the properties of $S^k(n)$ are reflected in its distance matrix A by going through the definitions

and theorems and rephrasing them in terms of A. Of course, one of the critical questions in this regard is whether these and other significant properties of A lend themselves to matric methods and theory. Also of value may be an investigation of the behaviour of subspaces of $S^k(n)$ under motions of $S^k(n)$. (Any circle of radius 1, $C = C(a, 1) = \{x; d(x, a) = 1\}$, is a metric basis for $S^k(n)$. Considering such a circle, it is not difficult to show that the group of motions of $S^k(n)$ is the semi-direct product of A by B, where A is the direct product of k symmetric groups on n letters, and B is the symmetric group on k letters.) For example, what can be said about the group of motions which carries an $L(n, k, r)$ space into itself?

In addition to these metric spaces being objects of interest in their own right, the results thus far obtained offer hope that this type of approach may provide a useful common orientation for a wide class of combinatorial problems.

Acknowledgments. The author wishes to express his sincere appreciation to his former adviser Professor D. R. Whitney for many helpful suggestions in the exposition, to Professors Marshall Hall, Jr., and H. B. Mann for taking time from their own busy schedules to lend a sympathetic ear, and most especially to Professors Whitney and H. J. Ryser for their continued encouragement. Finally, the author wishes to thank the referee for calling his attention to recent developments.

Addendum. Since the submission of this paper, there have been several developments in the field. The work of Bose, Parker, and Shrikhande has annihilated the Euler conjecture. It is now known that pairs of orthogonal Latin squares ($L(n, 4, 2)$ spaces) exist for all orders except $n = 2, 6$. It will be interesting to see to what extent their construction techniques can be extended to general $L(n, k, r)$ spaces. Remaining related problems are in a state of flux. Also, in a recent conversation the author learned from Professor Bose that the metric space $S^k(2)$ has been studied in connection with error correcting codes. (The metric space $S^k(2)$ is, of course, isometric with the set of vertices of a k-dimensional Euclidean hypercube of unit side, where the distance between vertices is taken as the square of the Euclidean distance. Also, $S^k(n)$ can be essentially embedded in $S^{kn}(2)$ in a trivial manner.) The elements are termed k-place messages and the metric is termed the Hamming distance. It is important in the theory of symmetric binary codes to determine the t-extent of $S^k(2)$. Discussion of this problem and additional bibliography can be found in **(28)**, along with an excellent summary of the status of the existence problem for Hadamard matrices. One of the main results in the above paper is that if we consider $(4t - 1)$-place messages having all mutual distances greater than or equal to $2t$, then the existence of the maximum number, $4t$, of such messages is equivalent to the existence of a symmetric BIBD with parameters $v = b = 4t - 1$, $r = k = 2t - 1$, $\lambda = t - 1$ (or

equivalently, to the existence of a Hadamard matrix of order $4t$). This result may also be obtained as a corollary to Theorem 4.2 of the present paper by taking $n = 2$, $k = 4t - 1$ and $r = 2t$. The design derived from the resolvable BIBD of the theorem by deleting one variety and all blocks not containing it, is precisely the symmetric BIBD obtained by Bose and Shrikhande. More generally, for $n = 2$, Theorem 4.2 may be rephrased: If we consider m-place messages having all mutual distances greater than or equal to d, then for $d + 1 \leqslant m < 2d$, the maximum number of such messages is less than or equal to $2d/(2d - m)$, and equality is attained if and only if there exists a BIBD with parameters

$$b = m,\ v = \frac{m}{2d - m},\ r = m - d,\ k = \frac{m - d}{2d - m},\ \lambda = \frac{2m - 3d}{2}.$$

References

1. Reinhold Baer, *Nets and groups*, Trans. Amer. Math. Soc., *46* (1939), 110–141.
2. W. W. Rouse Ball, *Mathematical Recreations and Essays* (New York, 1947).
3. Grace E. Bates, *Free loops and nets and their generalizations*, Amer. J. Math., *69* (1947), 499–550.
4. Leonard M. Blumenthal, *Distance geometries*, University of Missouri Studies, vol. 13, no. 2 (1938).
5. ——— *Theory and applications of distance geometry* (New York, 1953).
6. R. C. Bose, *On the application of the properties of Galois fields to the problem of construction of hyper-Graeco-Latin squares*, Sankhya, *3* (1938), 323–338.
7. R. C. Bose and K. A. Bush, *Orthogonal arrays of strength two and three*, Ann. Math. Stat., *23* (1952), 508–524.
8. K. A. Bush, *Orthogonal arrays of index unity*, Ann. Math. Stat., *23* (1952), 426–434.
9. R. H. Bruck, *Finite nets, I. Numerical invariants*, Can. J. Math., *3* (1951), 94–107.
10. R. H. Bruck and H. J. Ryser, *The nonexistence of certain finite projective planes*, Can. J. Math., *1* (1949), 88–93.
11. S. Chowla and H. J. Ryser, *Combinatorial problems*, Can. J. Math., *2* (1950), 93–99.
12. Leonard Euler, *Recherches sur une nouvelle espèce de quarrés magiques*, Commentationes Algebraicae, Opera Omnia, series prima, 7 (1923).
12.1 R. A. Fisher and F. Yates, *Statistical tables for Biological, agricultural, and medical research* (1st ed., Oliver and Boyd, 1938).
13. Marshall Hall, Jr., *Projective planes*, Trans. Amer. Math. Soc., *54* (1943), 229–277.
14. F. W. Levi, *Finite geometrical systems* (University of Calcutta, 1942).
15. A. Lindenbaum, *Contributions à l'étude de l'espèce métrique*, I Fund. Math. *8* 1926), 209–222.
16. H. F. MacNeish, *Euler squares*, Ann. Math., *23* (1921), 221–227.
17. H. B. Mann, *On orthogonal Latin squares*, Bull. Amer. Math. Soc., *50* (1944), 249–257.
18. ——— *Analysis and design of experiments* (New York, 1949).
19. H. W. Norton, *The 7 × 7 squares*, Ann. Eugen., *9* (1939), 269–307.
20. R. E. A. C. Paley, *On orthogonal matrices*, J. Math. and Phys., *12* (1933), 311–320.
21. C. R. Rao, *Hypercubes of strength d leading to confounded designs in factorial experiments*, Bull. Calcutta Math. Soc., *38* (1946) 67–78.
22. H. J. Ryser, *Geometries and incidence matrices*, Amer. Math. Monthly, *62* (1955), 25–31.
23. Esther Seiden, *On the problem of construction of orthogonal arrays*, Ann. Math. Stat., *25* (1954), 151–156.

24. W. L. Stevens, *The completely orthogonalized Latin square*, Ann. Eugen., *9* (1939), 82–93.
25. G. Tarry, *Le problème de 36 officiers*, Mathesis, *20* (1901).
26. F. Yates, *Incomplete randomized blocks*, Ann. Eugen., *7* (1936), 121–140.

Added in proof

27. R. C. Bose and S. S. Shrikhande, *On the falsity of Euler's conjecture about the non-existence of two orthogonal Latin squares of order $4t + 2$*, Proc. N. A. S., *45* (1959), 734–737.
28. ——— *A note on a result in the theory of code construction*, Inform. and Control, *2* (1959), 183–194.
29. ——— *On the falsity of Euler's conjecture for all orders exceeding 26*, Amer. Math. Soc. Notices, *6* (1959), 379.
30. R. W. Hamming, *Error detecting and error correcting codes*, Bell System Tech. J., *29* (1950), 147–160.
31. E. T. Parker, *Construction of some sets of pairwise orthogonal Latin squares*, Amer. Math. Soc. Notices, *5* (1958), 815.
32. ——— *Orthogonal Latin squares*, Proc. Nat. Acad. Sci., *45* (1959), 859–862.
33. ——— *Completion of disproof of Euler's conjecture*, Am. Math. Soc. Notices, *6* (1959), 391.
34. M. Plotkin, *Binary codes with specified minimum distance*, Research Div. Rept. 51–20, University of Pennsylvania.
35. R. R. Varsamov, *The evaluation of signals in codes with correction of errors*, Math. Rev., *20* (1959), 262.

Ohio State University
and
The National Bureau of Standards